School of Electrical Engineering and Computing
Department of Computing

The k-error Linear Complexity Distribution for Periodic Sequences

Jianqin Zhou

This thesis is presented for the Degree of
Doctor of Philosophy
of
Curtin University

January 2017

To the best of my knowledge and belief this thesis contains no material previously published by any other person except where due acknowledgement has been made. This thesis contains no material which has been accepted for the award of any other degree or diploma in any university.

Jianqin Zhou	Date

Abstract

Strong key stream sequences in cryptographic applications should not only have a high linear complexity but the linear complexity should also be stable. The concept of linear complexity and k-error linear complexity have attracted much attention in the cryptography research community. There has been some research on the k-error linear complexity distribution of 2^n-periodic binary sequences for $k \leq 3$. Several researchers have started to study CELCS (critical error linear complexity spectrum) for the k-error linear complexity distribution of 2^n-periodic binary sequences. There have been some results about the **first descent point** of k-error linear complexity.

The aim of this thesis is to propose several novel approaches, so that we can further study the k-error linear complexity distribution of 2^n-periodic binary sequences for $k > 3$, and the **second descent point and beyond** of k-error linear complexity critical error points. More importantly, with prescribed linear complexity and k-error linear complexity, we aim to give an approach to constructing all such 2^n-periodic binary sequences. This is a challenging problem with broad applications.

To further the study of the k-error linear complexity distribution for 2^n-periodic binary sequences, we propose a **framework** as follows. Let $S = \{s|L(s) = c\}, E = \{e|W_H(e) \leq w\}, S + E = \{s + e|s \in S, e \in E\}$, where s is a sequence with linear complexity c, e is an error sequence with $W_H(e) \leq w$. We aim to sieve sequences $s + e$ with $L_k(s + e) = c$ from $S+E$. By a **divide and conquer** method of combinatorics, we investigate sequences with linear complexity 2^n, and sequences with linear complexity less than 2^n, separately. With our approach, the issue to study k-error linear complexity distribution for 2^n-periodic binary sequences becomes a combinatorial problem of these subsequences.

With our framework along with the sieve method, for $k = 2, 3, 4$, the complete counting functions on the k-error linear complexity of 2^n-periodic binary sequences with both *linear complexity* 2^n and *linear complexity less than* 2^n are characterized. We also obtain some partial results about the 5-error linear complexity of 2^n-periodic binary sequences. On the other hand, we derive a full representation of the first descent point spectrum for the k-error linear complexity. We obtain the complete counting functions on the number of 2^n-periodic binary sequences with given 2^m-error linear complexity and linear complexity $2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m})$, where $0 \leq i_1 < i_2 < \cdots < i_m < n$.

The sequences with only two k-error linear complexity values exactly, namely its k-error linear complexity is only L(s) or 0, have been studied. Based on this concept, we present a new tool called the **Cube Theory**. It is proved that a binary sequence with period 2^n can be decomposed into some disjoint cubes. Based on the Games-Chan Algorithm, we propose **a standard cube decomposition** for any binary sequence with period 2^n. With such decomposition, we are capable to construct sequences with the maximum stable k-error linear complexity. It is also proved that the maximum k-error linear complexity is $2^n - (2^l - 1)$ over all 2^n-periodic binary sequences, where $2^{l-1} \leq k < 2^l$ and $l < n$.

By the cube theory, a new approach to determining the CELCS for the k-error linear complexity distribution of 2^n-periodic binary sequences is developed via the sieve method and Games-Chan algorithm. The **second descent point** distribution of the 3-error linear complexity, the second descent point distribution of the 4-error linear complexity and the **third descent point** distribution of the 5-error linear complexity for 2^n-periodic binary sequences are characterized completely.

Based on the Games-Chan algorithm and cube theory, a constructive approach is presented to **construct 2^n-periodic sequences with the given k-error linear complexity profile**. Consequently, the complete counting formula of 2^n-periodic binary sequences is derived with the given k-error linear complexity profile having descent points 1, 3, 5 and 7. The k-error linear complexity profile having descent points 2, 4, 6 and 8 is also partially discussed. The proposed constructive approach can be used to construct 2^n-periodic binary sequences with the given linear complexity and k-error linear complexity.

Most results in this thesis are presented along with examples, which are verified by computer program.

Acknowledgments

I would like to express my greatest gratitude to the following people for the great guidance and support during the long journey of my PhD study. This thesis would not be possible without them.

- First and foremost, I owe my deepest gratitude to my supervisor Associate Professor Wanquan Liu and co-supervisor Associate Professor Guanglu Zhou for their constant encouragement, guidance, and support through all my PhD study period. This study has been a very valuable learning experience in my life.

- I also greatly appreciate the support and care from my late wife Fengmei Zang, my daughter Baolin Zhou and other family members. Thank you so much for keep motivating and believing in me.

- I am really grateful to Mingliang Xue, Antoni Liang, Jinglan Tian, Chenyu Wang and Qilin Li for all the advices and suggestions during the years of my study.

- Special thanks go to Dr. Bin Ji for his advices and support during the years of my study.

- Lastly, I am particularly grateful to Curtin University for providing financial support for my PhD study through International Postgraduate Research Scholarship (IPRS).

Published Work

This is the list of all the published works (and under preparation) included in this thesis following the order of publication:

- Jianqin Zhou, Wanquan Liu and Guanglu Zhou. (2013) Cube Theory and Stable k-Error Linear Complexity for Periodic Sequences. *The 9th China International Conference on Information Security and Cryptology (INSCRYPT)*. LNCS 8567, pages 70-85. (Chapter 3)

- Jianqin Zhou and Wanquan Liu. (2014) The k-error Linear Complexity Distribution for 2^n-periodic Binary Sequences. *Designs, Codes and Cryptography*. 2014, 73(1), pages 55-75. (Chapter 2)

- Jianqin Zhou, Wanquan Liu and Xifeng Wang. (2015) Characterization of the Third Descent Points for the k-error Linear Complexity of 2^n-periodic Binary Sequences. *17th International Conference of Information and Communications Security (ICICS)*. LNCS 9543, pages 169-183. (Chapter 4)

- Jianqin Zhou, Wanquan Liu and Xifeng Wang. (2015) The Cube Theory for 2^n-Periodic Binary Sequences. *9th International Conference on Future Generation Communication and Networking (FGCN)*. pages 1-4. (Chapter 3)

- Jianqin Zhou, Wanquan Liu and Xifeng Wang. (2016) Cube Theory and k-error Linear Complexity Profile. *International Journal of Security and Its Applications (IJSIA)*. 2016, 10(7), pages 169-184.(Chapter 3 and 5)

- Jianqin Zhou, Wanquan Liu and Xifeng Wang. (2017) Structure Analysis on the k-error Linear Complexity for 2^n-periodic Binary Sequences. *Journal of Industrial and Management Optimization (JIMO)*, 2017, http://www.aimsciences.org/journals/pdfs.jsp?paperID=13434&mode=full. (Chapter 4)

- Jianqin Zhou, Wanquan Liu and Xifeng Wang. (Accepted) Complete Characterization of the First Descent Point Distribution for the k-error Linear Complexity of 2^n-periodic Binary Sequences. *Advances in Mathematics of Communication*. (Chapter 2)

- Jianqin Zhou, Wanquan Liu and Jun Liu. (Under Preparation) A Unified Approach for the k-error Linear Complexity Distribution of 2^n-periodic Binary Sequences. (Chapter 2)

Contents

List of Figures

List of Tables

Chapter 1

Introduction

With the rapid development of Internet and communication, safeguarding communication and authenticating data have become more and more important, and the need for cryptology research has become more necessary and urgent. Crypotology includes cryptography and cryptanalysis. The latter mainly deals with the investigation of how to crack encryption algorithms or their implementations. Cryptography is mainly the study of methods for securing communications and authenticating data. A stream cipher is one of the most important symmetric key ciphers where plaintext digits are combined with a pseudorandom cipher digit stream (keystream). Stream ciphers have historical and practical importance, and have been well investigated (Menezes *et al.*, 1996; Paar and Pelzl, 2010).

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. As the LFSR that generates a given sequence s can be determined using the Berlekamp-Massey algorithm (Massey, 1969) with only the first $2L(s)$ elements of the sequence, hence for cryptographic purposes sequences with high linear complexity are highly necessary. The concept of linear complexity is very useful in the study of stream cipher security for cryptographic applications and it has attracted much attention in the cryptography research community (Games and Chan, 1983; Ding *et al.*, 1991; Stamp and Martin, 1993; Salagean, 2005). But large linear complexity of the sequence (key stream) does not necessarily guarantee the security of a stream cipher. To make a stream cipher secure, one has to make the linear complexity of the sequence (key stream) not only large, but also stable. Otherwise, suppose that the linear complexity of the sequence (key stream) decreased drastically by only changing a few symbols, an attacker could modify the key stream and try to decrypt the result using the Berlekamp-Massey algorithm (Massey, 1969). If the resulting sequence differs from the actual key stream by only a few symbols, the attacker could extract a large part of the message. This observation gives rise to the stability of linear complexity of sequences.

As a measure on the linear complexity of sequences, the weight complexity was first introduced by Ding (1990). A further refined measure, called sphere complexity, was

defined in the monograph by Ding, Xiao and Shan in (Ding *et al.*, 1991). Stamp and Martin (1993) introduced the k-error linear complexity, which is in essence the same as the sphere complexity. Specifically, suppose that s is a sequence with period N. For any $k(0 \leq k \leq N)$, 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 bits of the sequence are changed within one period.

One important result, proved by Kurosawa *et al.* (2000), 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. According to Meidl (2004), for the period length p^n, where p is an odd prime and 2 is a primitive root modulo p^2, a relationship is established between the linear complexity and the minimum value k for which the k-error linear complexity is strictly less than the linear complexity. For generalization of these results by Zhou (2011), 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.

Rueppel (2012) derived the number of 2^n-periodic binary sequences with given linear complexity $L, 0 \leq L \leq 2^n$. For $k = 1, 2$, Meidl (2005) characterized the complete counting functions on the k-error linear complexity of 2^n-periodic binary sequences with linear complexity 2^n. For $k = 2, 3$, Zhu and Qi (2007) further gave the complete counting functions on the k-error linear complexity of 2^n-periodic binary sequences with linear complexity $2^n - 1$. By using algebraic and combinatorial methods, Fu *et al.* (2006) characterized the 2^n-periodic binary sequences with the 1-error linear complexity and derived the counting function completely for the 1-error linear complexity of 2^n-periodic binary sequences.

By investigating sequences with linear complexity 2^n and linear complexity less than 2^n together, Kavuluru (2008, 2009) characterized 2^n-periodic binary sequences with the 2-error and 3-error linear complexity, and obtained the counting functions for the number of 2^n-periodic binary sequences with the k-error linear complexity for $k = 2$ and 3. By Zhou (2012), it is proved with one counterexample that the counting functions by Kavuluru (2008, 2009) for the number of 2^n-periodic binary sequences with the 3-error linear complexity are incorrect in some cases.

As the LFSR that generates a given sequence s can be determined using the Berlekamp-Massey algorithm (Massey, 1969) with only the first $2L(s)$ elements of the sequence, hence a cryptographically strong sequence must have both larger linear complexity and

k-error linear complexity. Due to the importance of linear complexity and k-error linear complexity in the study of stream cipher security for cryptographaic applications, many researchers have studied the CELCS (critical error linear complexity spectrum) for the k-error linear complexity distribution of 2^n-periodic binary sequences (Kurosawa *et al.*, 2000; Lauder and Paterson, 2003; Salagean, 2005; Etzion *et al.*, 2009; Pi and Qi, 2011). Recently, by using short sequences to construct longer sequences in a manner similar to the reversed process of the Games-Chan algorithm (Games and Chan, 1983), Pan *et al.* (2016) investigated the distribution of linear complexity and k-error linear complexity of 2^n-periodic binary sequences with fixed Hamming weight.

1.1 Aims and Research Goals

After some investigations, we discovered some research gaps and directions that we want to address:

1. The concept of linear complexity and k-error linear complexity have attracted much attention in the cryptography research community. There has been some research on the k-error linear complexity distribution of 2^n-periodic binary sequences for $k \leq 3$. Algebra (Meidl, 2004, 2005; Fu *et al.*, 2006; Zhu and Qi, 2007) and discrete Fourier transform (Meidl and Niederreiter, 2002; Hu and Feng, 2005) are two important tools to study the k-error linear complexity for periodic sequences. To further the study of the k-error linear complexity distribution for 2^n-periodic binary sequences, we need some novel approaches.

2. Several researchers have studied the CELCS (critical error linear complexity spectrum) for the k-error linear complexity distribution of 2^n-periodic binary sequences (Lauder and Paterson, 2003; Etzion *et al.*, 2009). There have been only some results about the **first descent point** of k-error linear complexity (Kurosawa *et al.*, 2000; Lauder and Paterson, 2003; Etzion *et al.*, 2009). With the current techniques, it is extremely difficult to study the **second descent point and beyond** of k-error linear complexity critical error points. We should cope with a sequence from different perspectives and need some new techniques.

3. The motivation of studying the stability of linear complexity is that changing a small number of elements in a sequence may lead to a sharp decline of its linear complexity (Ding, 1990; Ding *et al.*, 1991; Niu *et al.*, 2013, 2014). Therefore we really need to study such stable sequences in which even a small number of changes do not reduce

their linear complexity. We should study how to construct sequences with stable k-error linear complexity. It is also important to construct periodic sequences with prescribed linear complexity and k-error linear complexity. This is a challenging problem with broad applications.

1.2 Preliminaries for Linear Complexity

In this section we give some preliminary results which will be used in the sequel.

We consider sequences over $GF(q)$, which is the finite field of order q. If there exists a positive integer N such that $s_i = s_i + N$ for $i = 0, 1, 2, \cdots$, then s is called a periodic sequence, and N is called the period of s.

Let $x = (x_1, x_2, \cdots, x_n)$ and $y = (y_1, y_2, \cdots, y_n)$ be vectors over $GF(q)$. Define $x + y = (x_1 + y_1, x_2 + y_2, \cdots, x_n + y_n)$, which is called as the superposition of x and y.

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 in each period of s, denoted by $W(s)$. Let s^N be one period of s. If $N = 2^n$, s^N is also denoted as $s^{(n)}$. Obviously, $W(s^{(n)}) = W(s^N) = W(s)$. $supp(s)$ is defined as the set of the positions with nonzero elements in each period of s. The distance of two elements is defined as the difference of their indexes. For instance, the distance of x_1, x_3 in $x = (x_1, x_2, x_3, \cdots, x_n)$ is 3-1=2.

Let $s = \{s_0, s_1, s_2, s_3, \cdots, \}$ be a sequence over $GF(q)$. The sequence s is called an K-order linear recursive sequence if there exists a positive number K and $c_1, c_2, \cdots, c_K$ in $GF(q)$ such that $s_j + c_1 s_{j-1} + \cdots + c_K s_{j-K} = 0$ for any $j \geq K$. The minimal order is called the linear complexity of s, which is denoted by $L(s)$.

The generating function of a sequence $s = \{s_0, s_1, s_2, s_3, \cdots, \}$ is defined by

$$s(x) = s_0 + s_1 x + s_2 x^2 + s_3 x^3 + \cdots = \sum_{i=0}^{\infty} s_i x^i$$

The generating function of a finite sequence $s^N = \{s_0, s_1, s_2, \cdots, s_{N-1}\}$ is defined by $s^N(x) = s_0 + s_1 x + s_2 x^2 + \cdots + s_{N-1} x^{N-1}$. If s is a periodic sequence with the first period

s^N, then,

$$\begin{aligned} s(x) &= s^N(x)(1 + x^N + x^{2N} + \cdots) = \frac{s^N(x)}{1 - x^N} \\ &= \frac{s^N(x)/\gcd(s^N(x), 1 - x^N)}{(1 - x^N)/\gcd(s^N(x), 1 - x^N)} = \frac{g(x)}{f_s(x)} \end{aligned}$$

Obviously, $\gcd(g(x), f_s(x)) = 1, \deg(g(x)) < \deg(f_s(x))$. $f_s(x)$ is called the minimal polynomial of s, and the degree of $f_s(x)$ is called the linear complexity of s, that is $\deg(f_s(x)) = L(s)$ (Ding *et al.*, 1991).

Suppose that $N = 2^n$ and $GF(q) = GF(2)$. Then $1-x^N = 1-x^{2^n} = (1-x)^{2^n} = (1-x)^N$. If s is a binary sequence with period 2^n, its linear complexity is N minus the degree of factor $(1-x)$ in $s^N(x)$. This is the foundation of the Games-Chan algorithm (Games and Chan, 1983) for the linear complexity of a 2^n-periodic binary sequence.

1.3 Thesis Structure and Contributions

The list below briefly describes the content of each chapter in this thesis along with its contributions.

- Chapter 2: We propose a **structural approach** for determining the k-error linear complexity distribution for 2^n-periodic binary sequences (Zhou and Liu, 2014). We mainly use the **sieve approach** and the Games-Chan algorithm (Games and Chan, 1983). Furthermore, by a **divide and conquer** method of combinatorics, we investigate sequences with linear complexity 2^n, and sequences with linear complexity less than 2^n, separately. In this way, the issue to study k-error linear complexity distribution for 2^n-periodic binary sequences becomes a combinatorial problem of these subsequences. With our structural approach along with the sieve method, for $k = 2, 3, 4$, the complete counting functions on the k-error linear complexity of 2^n-periodic binary sequences with both *linear complexity* 2^n and *linear complexity less than* 2^n are characterized. We also obtain some partial results about the 5-error linear complexity of 2^n-periodic binary sequences. Additionally, to verify the theorem in Chapter 2, for $n = 5$, the numbers of 2^n-periodic binary sequences with linear complexity less than 2^n and the 4-error linear complexity c, $0 \leq c < 2^n$, are presented, and these results are also checked by a computer program.

  Finally, the first descent point (critical point) distribution of the k-error linear

complexity for 2^n-periodic binary sequences was characterized completely. We obtained the complete counting functions on the 2^m-error linear complexity of 2^n-periodic binary sequences with linear complexity $2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m})$, where $0 \leq i_1 < i_2 < \cdots < i_m < n$.

- Chapter 3: We begin by presenting a new concept of **stable k-error linear complexity**(Zhou *et al.*, 2013). The sequences with only two k-error linear complexity values exactly, namely its k-error linear complexity is only L(s) or 0, have been studied by Etzion *et al.* (2009). Based on this concept, we present a new tool called the **Cube Theory**(Zhou *et al.*, 2013, 2015b). First, it is proved that a binary sequence with period 2^n can be decomposed into some disjoint cubes. Second, based on the Games-Chan Algorithm, we propose **a standard cube decomposition** for any binary sequence with period 2^n. The main approaches of Chapter 4 and Chapter 5 are based on the cube decomposition theory. Finally, it is proved that the maximum k-error linear complexity is $2^n - (2^l - 1)$ over all 2^n-periodic binary sequences, where $2^{l-1} \leq k < 2^l$ and $l < n$. As a consequence of these results, some results by Niu *et al.* (2013, 2014) are proved to be incorrect. With such decomposition, some approaches are also presented to construct sequences with the maximum stable k-error linear complexity.

- Chapter 4: By the cube theory, a new structural approach to determining the CELCS for the k-error linear complexity distribution of 2^n-periodic binary sequences is developed (Zhou *et al.*, 2015a). Similar to Chapter 2, we also use the sieve approach and the Games-Chan algorithm (Games and Chan, 1983). The structural approach is also based on the proposed framework in Chapter 2. First, we present the **second descent point** distribution of the 3-error linear complexity. Further, we investigate the second descent point distribution of the 4-error linear complexity. Furthermore, the **third descent point** distribution of the 5-error linear complexity for 2^n-periodic binary sequences are characterized completely.

  Finally, the k-error cube decomposition of 2^n-periodic binary sequences is developed based on **the Cube Theory** of Chapter 3. As an extension of the work by Kurosawa *et al.* (2000), we investigate the formulas to determine the second descent points and third descent points for the k-error linear complexity, respectively. Most results in Chapter 4 are presented along with examples, which are verified by computer program.

- Chapter 5: Based on the Games-Chan algorithm (Games and Chan, 1983) and the cube theory, a constructive approach is presented to **construct 2^n-periodic**

sequences with the given k-error linear complexity profile (Zhou *et al.*, 2016). Consequently, the complete counting formula of 2^n-periodic binary sequences is derived with the given k-error linear complexity profile having descent points 1, 3, 5 and 7. The k-error linear complexity profile having descent points 2, 4, 6 and 8 is also partially discussed. The proposed constructive approach can be used to construct 2^n-periodic binary sequences with the given linear complexity and k-error linear complexity. Lastly, to verify the results in Chapter 5, we give the complete 2^n-periodic binary sequence distribution with the given k-error linear complexity profile of $0 = L_7(s^{(n)}) < L_5(s^{(n)}) < L_3(s^{(n)}) < L_1(s^{(n)}) < L(s^{(n)}) = 2^n$ for $n = 5$, which is checked by a computer program.

- Chapter 6: The **conclusion** of the whole thesis and some **potential future directions** are addressed.

Chapter 2

A Unified Approach for the k-error Linear Complexity Distribution of 2^n-periodic Binary Sequences

By investigating sequences with linear complexity 2^n and linear complexity less than 2^n together, Kavuluru (2008, 2009) obtained the counting functions for the number of 2^n-periodic binary sequences with k-error linear complexity for $k = 2$ and 3. By Zhou (2012), it is proved with one counterexample that the counting functions by Kavuluru (2008, 2009) for the number of 2^n-periodic binary sequences with the 3-error linear complexity are incorrect in some cases.

In this thesis, we propose a structural approach for determining the k-error linear complexity distribution for 2^n-periodic binary sequences (Zhou and Liu, 2014). We mainly use the sieve approach and the Games-Chan algorithm (Games and Chan, 1983). The proposed approach is different from those by Meidl (2005); Fu *et al.* (2006) and Zhu and Qi (2007), and it is based on the following framework.

Let $S = \{s|L(s) = c\}, E = \{e|W_H(e) = k\}, S + E = \{s + e|s \in S, e \in E\}$, where s and e are two sequences. We aim to sieve sequences $s+e$ with $L_k(s+e) = c$ from $S+E$. For this purpose, we need to investigate two cases. One is to exclude all sequences $s + u \in S + E$, with $L_k(s + u) < c$. Based on Lemma 2.1.2 in Section 2.1, this is equivalent to checking if there exists a sequence v such that $L(u+v) = c$. The other case is to check the repetition of some sequences in $S+E$ satisfying that $s+u, t+v \in S+E$ and $L_k(s+u) = L_k(t+v) = c$ with $s \neq t$, $u \neq v$, but $s + u = t + v$. Similarly, this is equivalent to checking if there exists a sequence v such that $L(u + v) = L(s + t) < c$ and if so, check the number of such sequences. With the sieve method of combinatorics, we attempt to sieve sequences $s + e$ with $L_k(s + e) = c$ in $S + E$. This is the first contribution of our **Unified Approach**.

The second contribution of our **Unified Approach** can be summarized as follows. First we investigate sequences with linear complexity 2^n, and sequences with linear complexity

less than 2^n, separately. It is observed that for sequences with linear complexity 2^n, the k-error linear complexity is equal to the $(k+1)$-error linear complexity, when k is odd. For sequences with linear complexity less than 2^n, the k-error linear complexity is equal to $(k+1)$-error linear complexity, when k is even. Based on these observations we investigate the k-error linear complexity in two cases and this would reduce the complexity of this problem. Finally, by combining the results of two cases, we obtain the complete counting functions for the number of 2^n-periodic binary sequences with the k-error linear complexity.

With our **Unified Approach**, the issue to study k-error linear complexity distribution for 2^n-periodic binary sequences becomes a combinatorial problem of these subsequences. With developed counting techniques, 3-error and 4-error linear complexity distribution for 2^n-periodic binary sequences is solved completely and other cases are investigated briefly for partial solutions. In this process, the most difficult part for the problem of the k-error linear complexity distribution is to calculate all the possible combinations of these subsequences, which becomes extremely complicated for large k.

Generally, the complete counting functions for the number of 2^n-periodic binary sequences with the k-error linear complexity for $k > 2$ could be possibly solved using our **Unified Approach**. However, the decomposition of the sequences is much more complex for larger k. For 3-error linear complexity being equal to $2^{n-1} - 2^{n-m}$, there are only 4 cases in the sieving process. In contrast, for 4-error linear complexity being equal to $2^{n-1} - (2^{n-m} + 2^{n-j})$, there are more than 10 cases in the sieving process. It remains for us to solve two difficult issues here. One is that the number of possible cases, which is related to $j - m$, is not a constant. The other is that we have to calculate the number of elements with more than 2 overlapped cases by using *the inclusion-exclusion principle* (Dohmen, 1999) in combinatorics.

The rest of this chapter is organized as follows. In Section 2.1, we first give an outline about our main approach for determining the k-error linear complexity distribution for 2^n-periodic binary sequences for $k = 2, 3, 4, 5, 6$ and 7. In Section 2.2, for $k = 2$, the counting functions on the k-error linear complexity of 2^n-periodic binary sequences with *linear complexity less than* 2^n are characterized. In Section 2.3, for $k = 3$, the counting functions on the k-error linear complexity of 2^n-periodic binary sequences with *linear complexity* 2^n are characterized. In Section 2.4, for $k = 2, 3$, the complete counting functions on the k-error linear complexity of 2^n-periodic binary sequences with both *linear complexity* 2^n and *linear complexity less than* 2^n are characterized. In Section 2.5, for $k = 4$, the counting functions on the k-error linear complexity of 2^n-periodic binary sequences with *linear complexity less than* 2^n are characterized. Finally in Section 2.6, for $k = 5$, the

counting functions on the k-error linear complexity of 2^n-periodic binary sequences with *linear complexity* 2^n are partially characterized.

2.1 Preliminaries

In this section we give some preliminary results which will be used in the sequel.

The linear complexity of a 2^n-periodic binary sequence s can be recursively computed by the Games-Chan algorithm (Games and Chan, 1983) as follows.

Algorithm 2.1.1

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 $Left(s) \bigoplus Right(s)$ recursively. Namely, $L(s) = 2^{n-1} + L(Left(s) \bigoplus Right(s))$.

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

Remark 2.1.1 Based on this algorithm, one can see that the linear complexity of a sequence s is in the following form

$$L(s) = 2^{n-1} + 2^{n-2} + \cdots + 2 + 1 + 1 - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m}) = 2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m}),$$

where i_k represents the case that $Left(s) = Right(s)$ in the loop $n - i_k$ with $0 \leq i_1 < i_2 < \cdots < i_m < n$. Conversely, with a given linear complexity value in above form, one can construct a sequence s such that its linear complexity equals to this value.

The following three lemmas are well known results on 2^n-periodic binary sequences. Please

refer to Meidl (2005); Zhu and Qi (2007) for details.

Lemma 2.1.1 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 element 0 in each period of a sequence with odd Hamming weight, the Hamming weight of the sequence will be changed to even, so the main concern hereinafter is about sequences with even Hamming weight.

Lemma 2.1.2 Let s_1 and s_2 be two binary sequences with period $N = 2^n$. If $L(s_1) \neq L(s_2)$, 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 least k elements of s are changed. We construct a binary sequence e, in which only elements at exactly those k changed positions are nonzeros. By Lemma 2.1.2, the linear complexity of the binary sequence e must be $L(s)$. Therefore, for computation of the k-error linear complexity, we need to first find the binary sequence with the minimal Hamming weight and its linear complexity is $L(s)$.

Lemma 2.1.3 Let E_i be a 2^n-periodic sequence with one nonzero element at position i and 0 elsewhere in each period, $0 \leq i < 2^n$. If $j - i = 2^r(1 + 2a), a \geq 0, 0 \leq i < j < 2^n, r \geq 0$, then $L(E_i + E_j) = 2^n - 2^r$.

We have the following result on the linear complexity of sequences with Hamming weight less than 8.

Lemma 2.1.4 Suppose that s is a binary sequence with period 2^n and the Hamming weight is $w < 8$. Then the linear complexity of s is $L(s) = 2^n - 2^{n-m}, 1 < m \leq n$ or $2^n - (2^{n-m} + 2^{n-j})$, $1 \leq m < j \leq n$.

Proof. Suppose that s is a 2^n-periodic binary sequence with $W_H(s) = w < 8$. If the linear complexity of s is neither $2^n - 2^{n-m}$ nor $2^n - (2^{n-m} + 2^{n-j})$, then the minimum number k for which the k-error linear complexity of s is strictly less than the linear complexity $L(s)$, can be given by $k_{\min} = 2^{W_H(2^n - L(s))} \geq 8$, where $W_H(b)$ denotes the Hamming weight of the binary representation of an integer b. This contradicts the fact that the w-error linear complexity of the binary sequence s is 0 ($L_w(s) = 0$). So the linear complexity of s must be $2^n - 2^{n-m}, 1 < m \leq n$ or $2^n - (2^{n-m} + 2^{n-j})$, $1 \leq m < j \leq n$. □

Based on the Games-Chan algorithm, the following lemma is given by Meidl (2005).

Lemma 2.1.5 Suppose that s is a binary sequence with one period $s^{(n)} = \{s_0, s_1, s_2, \cdots, s_{2^n-1}\}$, a mapping φ_n from $F_2^{2^n}$ to $F_2^{2^{n-1}}$ is defined as

$$\begin{aligned} \varphi_n(s^{(n)}) &= \varphi_n((s_0, s_1, s_2, \cdots, s_{2^n-1})) \\ &= (s_0 + s_{2^{n-1}}, s_1 + s_{2^{n-1}+1}, \cdots, s_{2^{n-1}-1} + s_{2^n-1}). \end{aligned}$$

Let $W_H(\upsilon)$ denote the Hamming weight of a vector υ. Then the mapping φ_n has the following properties.

1) $W_H(\varphi_n(s^{(n)})) \leq W_H(s^{(n)})$;

2) If $n \geq 2$, then $W_H(\varphi_n(s^{(n)}))$ and $W_H(s^{(n)})$ are either both odd or both even;

3) The set

$$\varphi_{n+1}^{-1}(s^{(n)}) = \{v \in F_2^{2^{n+1}} | \varphi_{n+1}(v) = s^{(n)}\}$$

of the preimage of $s^{(n)}$ has cardinality 2^{2^n}.

Rueppel (2012) presented the following result on the number of sequences with a given linear complexity.

Lemma 2.1.6 The number $N(L)$ of 2^n-periodic binary sequences with linear complexity $L, 0 \leq L \leq 2^n$, is given by $N(L) = \begin{cases} 1, & L = 0 \\ 2^{L-1}, & 1 \leq L \leq 2^n \end{cases}$

In this thesis, we will investigate sequences with *linear complexity* 2^n, and sequences with *linear complexity less than* 2^n, separately. It is observed that for sequences with *linear complexity* 2^n, the k-error linear complexity is equal to $(k+1)$-error linear complexity, when k is odd. For sequences with *linear complexity less than* 2^n, the k-error linear complexity is equal to $(k+1)$-error linear complexity, when k is even. Therefore, in order to characterize 2^n-periodic binary sequences with the 3-error linear complexity, we need first to consider the 2^n-periodic binary sequences with *linear complexity less than* 2^n and the 2-error linear complexity, and we will also fully characterize the 2^n-periodic binary sequences with *linear complexity* 2^n and the 3-error linear complexity.

Similarly, in order to characterize 2^n-periodic binary sequences with the 4-error linear complexity, we need first to consider the 2^n-periodic binary sequences with *linear complexity* 2^n and the 3-error linear complexity, and then characterize the 2^n-periodic binary

sequences with *linear complexity less than* 2^n and the 4-error linear complexity.

Further, in order to characterize 2^n-periodic binary sequences with the prescribed 5-error linear complexity, we can first consider 2^n-periodic binary sequences with *linear complexity less than* 2^n and the prescribed 4-error linear complexity, and then we need consider 2^n-periodic binary sequences with *linear complexity* 2^n and the prescribed 5-error linear complexity. In this thesis, only partial results are given here based on the proposed framework.

Of course, one can extend this idea to characterize 2^n-periodic binary sequences with the k-error linear complexity for $k = 6, 7$.

The proposed structural approach is based on the following framework. Let $S = \{s|L(s) = c\}, E = \{e|W_H(e) \leq w\}, S + E = \{s + e|s \in S, e \in E\}$, where s is a sequence with linear complexity c, $w < 8$ and e is an error sequence (Kaida *et al.*, 1999) with $W_H(e) \leq w$. Note that the number of 2^n-periodic binary sequences in E is $1 + 2^n + \binom{2^n}{2} + \cdots + \binom{2^n}{w}$. By Lemma 2.1.6, the number of 2^n-periodic binary sequences $s + e \in S + E$ is at most $(1 + 2^n + \binom{2^n}{2} + \cdots + \binom{2^n}{w})2^{c-1}$. With the sieve method, we aim to sieve sequences $s + e$ with $L_w(s + e) = c$ from $S + E$.

Intuitively, we aim to characterize the 2^n-periodic binary sequences with *linear complexity less than* 2^n and the 4-error linear complexity. If $W_H(e) = 1$ or 3, then $W_H(s + e)$ is odd, thus $L(s + e) = 2^n$. As we only consider the binary sequences with *linear complexity less than* 2^n, so we can only consider the error sequences with $W_H(e) = 0$ or 2 or 4. In the same way, when we characterize the 2^n-periodic binary sequences with *linear complexity* 2^n and the 5-error linear complexity. If $W_H(e) = 0, 2$ or 4, then $W_H(s + e)$ is odd, thus $L(s + e) = 2^n$. As we only consider binary sequences with *linear complexity* 2^n, so we can only consider the error sequences with $W_H(e) = 1$ or 3 or 5.

Given a 2^n-periodic binary sequence $s^{(n)}$, based on the Games-Chan algorithm (Games and Chan, 1983), its linear complexity is either 0 or $L(r, c) = 2^{n-1} + 2^{n-2} + \cdots + 2^r + c = 2^n - 2^r + c$, $2 \leq r \leq n, 1 \leq c < 2^{r-1}$. With the following result, we only need to consider 2^r-periodic binary sequences $s^{(r)}$ with *linear complexity* c.

Lemma 2.1.7 Suppose that $s^{(n)}$ is a binary sequence with period 2^n and its linear complexity is either 0 or $L(r, c) = 2^{n-1} + 2^{n-2} + \cdots + 2^r + c = 2^n - 2^r + c$, $2 \leq r \leq n, 1 \leq c \leq 2^{r-1} - 1$. Let $u^{(r)}$ be a binary sequence with period 2^r and $W_H(u^{(r)}) = k$, and $u^{(n)}$

be a binary sequence with period 2^n constructed by adding zero elements to $u^{(r)}$. Then $L_k(s^{(r)} + u^{(r)}) = c \Leftrightarrow L_k(s^{(n)} + u^{(n)}) = L(r, c)$, where $s^{(r)} = \varphi_{r+1} \cdots \varphi_n(s^{(n)})$.

Proof. Let $v^{(r)}$ be a binary sequence with period 2^r and $W_H(v^{(r)}) \leq k$, such that $L(u^{(r)} + v^{(r)}) = c$. Let $v^{(n)}$ be a binary sequence with period 2^n constructed by adding zero elements to $v^{(r)}$. Then $L(u^{(n)} + v^{(n)}) = 2^{n-1} + 2^{n-2} + \cdots + 2^r + c = 2^n - 2^r + c = L(r, c)$.

On the contrary, let $v^{(n)}$ be a binary sequence with period 2^n and $W_H(v^{(n)}) \leq k$, such that $L(u^{(n)}+v^{(n)}) = L(r, c)$. Based on the Games-Chan algorithm, $u^{(r)}+v^{(r)} = \varphi_{r+1} \cdots \varphi_n(u^{(n)}+ v^{(n)})$ and $L(u^{(r)} + v^{(r)}) = c$, where $v^{(r)} = \varphi_{r+1} \cdots \varphi_n(v^{(n)})$.

By Lemma 2.1.2, we have proved that $L_k(s^{(r)} + u^{(r)}) < c \Leftrightarrow L_k(s^{(n)} + u^{(n)}) < L(r, c)$.

This completes the proof. □

By Lemma 2.1.7, in order to characterize 2^n-periodic binary sequences with the k-error linear complexity, we just need to consider the k-error linear complexity for $0 \leq c < 2^{n-1}$. For such purpose, we first consider a simple case.

Lemma 2.1.8 Suppose that $s^{(n)}$ and $t^{(n)}$ are two different binary sequences with linear complexity $c, 1 \leq c \leq 2^{n-3}$, and $u^{(n)}$ and $v^{(n)}$ are two different binary sequences with $W_H(u^{(n)}) < 8$, $W_H(v^{(n)}) < 8$. Then $s^{(n)} + u^{(n)} \neq t^{(n)} + v^{(n)}$.

Proof. First we observe the following fact

$$s^{(n)} + u^{(n)} \neq t^{(n)} + v^{(n)} \Leftrightarrow s^{(n)} + u^{(n)} + v^{(n)} \neq t^{(n)} \Leftrightarrow u^{(n)} + v^{(n)} \neq s^{(n)} + t^{(n)}$$

Note that $s^{(n)}$ and $t^{(n)}$ are two different binary sequences with linear complexity $c, 1 \leq c \leq 2^{n-3}$, so the linear complexity of $s^{(n)} + t^{(n)}$ is less than 2^{n-3}, hence one period of $s^{(n)} + t^{(n)}$ can be divided into 8 equal parts.

Suppose that $u^{(n)} + v^{(n)} = s^{(n)} + t^{(n)}$. Then one period of $u^{(n)} + v^{(n)}$ can be divided into 8 equal parts. As $W_H(u^{(n)}) < 8$, $W_H(v^{(n)}) < 8$, thus $u^{(n)} + v^{(n)}$ has 8 nonzero elements. It follows that the linear complexity of $u^{(n)} + v^{(n)}$ is 2^{n-3}, which contradicts the fact that the linear complexity of $s^{(n)} + t^{(n)}$ is less than 2^{n-3}. □

Now we need to consider more complicated cases with linear complexity $2^{n-3} < c < 2^{n-1}$.

First we have the following result.

Lemma 2.1.9 1). Suppose that $s^{(n)}$ is a binary sequence with linear complexity $c, 1 \leq c \leq 2^{n-1}-3$, $c \neq 2^{n-1}-2^{n-m}, 1 < m < n-1$ and $c \neq 2^{n-1}-(2^{n-m}+2^{n-j}), 1 < m < j \leq n$; $u^{(n)}$ is a binary sequence with $W_H(u^{(n)}) \leq k, 4 \leq k < 8$. Then the k-error linear complexity of $s^{(n)} + u^{(n)}$ is still c.

2). If $s^{(n)}$ is a binary sequence with linear complexity $c = 2^{n-1} - 2^{n-m}, 1 < m \leq n$ or $c = 2^{n-1} - (2^{n-m} + 2^{n-j}), 1 < m < j \leq n$. Then there exists a binary sequence $u^{(n)}$ with $W_H(u^{(n)}) \leq k, 4 \leq k < 8$, such that the k-error linear complexity of $s^{(n)} + u^{(n)}$ is less than c.

Proof. Suppose that $v^{(n)} \neq u^{(n)}$, and $W_H(v^{(n)}) \leq k$.

1). As $1 \leq c \leq 2^{n-1} - 3$, we only need to consider the case $L(u^{(n)} + v^{(n)}) < 2^{n-1}$. In this case, $LH(u^{(n)} + v^{(n)}) = RH(u^{(n)} + v^{(n)})$ and $W_H(LH(u^{(n)} + v^{(n)})) < 8$. By Lemma 2.1.3 and Lemma 2.1.4, one can obtain that $L(u^{(n)} + v^{(n)}) = 2^{n-1} - 2^{n-m}$, or $2^{n-1} - (2^{n-m} + 2^{n-j})$.

Thus $L(s^{(n)} + u^{(n)} + v^{(n)}) \geq L(s^{(n)})$, so the k-error linear complexity of $s^{(n)} + u^{(n)}$ is still c.

2). Note that $s^{(n)}$ is a binary sequence with linear complexity $c = 2^{n-1} - 2^{n-m}, 1 < m \leq n$ or $c = 2^{n-1} - (2^{n-m} + 2^{n-j}), 1 < m < j \leq n$. As seen from part 1), there exist $u^{(n)}$ and $v^{(n)}$ such that $L(u^{(n)} + v^{(n)}) = c$. So the k-error linear complexity of $s^{(n)} + u^{(n)}$ must be less than c □

Now by Lemma 2.1.9, we need only to consider the following three cases.

i) $c = 2^{n-1} - 2^{d_1} - 2^{d_2}, 0 \leq d_2 < d_1 \leq n - 2$.

ii) $c = 2^{n-1} - 2^{d_1} - 2^{d_2} + x, 0 \leq d_2 < d_1 \leq n - 2, 0 < x < 2^{d_2-1}$.

iii) $c = 2^{n-1} - 2^{d_1}, 0 \leq d_1 \leq n - 2$.

For a given linear complexity c, it remains for us to investigate two cases. One is that

$s+u \in S+E$, but $L_w(s+u) < c$. This is equivalent to checking if there exists a sequence v such that $L(u+v) = c$. We define $LESS = \{u | u \in E, v \in E, L(u+v) = c\}$. In this case, we first characterize the set $LESS$, then exclude such elements $s+e$ from the set $S+E$. The other is the case that $s+u, t+v \in S+E$ and $L_w(s+u) = L_w(s+v) = c$ with $s \neq t$, $u \neq v$, but $s+u = t+v$. It is equivalent to checking if there exists a sequence v such that $L(u+v) = L(s+t) < c$ and if so, check the number of such sequences v, where $W_H(u) \leq w, W_H(v) \leq w$. We define $EQUAL = \{u | u \in E, v \in E, L(u+v) < c\}$. In this case, we first characterize the set $EQUAL$, then take out these repetitions from the set $S+E$. This technique will be used in different places throughout this thesis.

In the next section, we will first fully characterize the 2-error linear complexity distribution of 2^n-periodic binary sequences with *linear complexity less than* 2^n.

2.2 Counting Functions with the 2-error Linear Complexity

For a 2^n-periodic binary sequence with linear complexity less than 2^n, the change of one bit in each period results in a sequence with odd number of nonzero bits in each period, which has linear complexity 2^n. In this section, we thus focus on the 2-error linear complexity.

Furthermore, the change of 1 bit or 3 bits in each period results in a sequence with odd number of nonzero bits in each period, which has linear complexity 2^n. In order to derive the counting functions of the 3-error linear complexity for 2^n-periodic binary sequences with linear complexity less than 2^n, we only need to investigate the 2-error linear complexity of 2^n-periodic binary sequences with linear complexity less than 2^n.

The main result of this section is the following theorem.

Theorem 2.2.1 Let $L(r,c) = 2^n - 2^r + c$, $2 \leq r \leq n, 1 \leq c \leq 2^{r-1} - 1$, and $N_2(L)$ be the number of 2^n-periodic binary sequences with linear complexity less than 2^n and the 2-error linear complexity L. Then

$$N_2(L) = \begin{cases} \binom{2^n}{2} + 1, & L = 0 \\ 2^{L-1}(\binom{2^r}{2} + 1), & L = L(r,c), 1 \le c \le 2^{r-2} - 1, r > 2 \\ 2^{L-1}(\binom{2^r}{2} + 1 - 3 \times 2^{r+m-3}), & \\ \qquad L = L(r,c), c = 2^{r-1} - 2^{r-m}, 1 < m \le r, r \ge 2 & \\ 2^{L-1}(\binom{2^r}{2} + 1 + 2^{r-m} - 2^{r+m-2}), & \\ \qquad L = L(r,c), c = 2^{r-1} - 2^{r-m} + x, 1 < m < r-1, 0 < x < 2^{r-m-1}, r > 3 & \\ 0, & \text{otherwise} \end{cases}$$

In order to prove Theorem 2.2.1, we first prove the following lemmas.

Lemma 2.2.1 1). If $s^{(n)}$ is a binary sequence with linear complexity $c, 1 \le c \le 2^{n-1} - 3$, $c \ne 2^{n-1} - 2^m, 2 \le m < n-1$, $u^{(n)}$ is a binary sequence with $W(u^{(n)}) = 0$ or 2. Then the 2-error linear complexity of $s^{(n)} + u^{(n)}$ is c.

2). If $s^{(n)}$ is a binary sequence with linear complexity $c = 2^{n-1} - 2^m, 0 \le m < n-1$. Then there exists a binary sequence $u^{(n)}$ with $W(u^{(n)}) = 2$, such that the 2-error linear complexity of $s^{(n)} + u^{(n)}$ is less than c.

Proof. Let $v^{(n)}$ be a binary sequence with $v^{(n)} \ne u^{(n)}$, and $W(v^{(n)}) = 0$ or 2.

1). As $c \le 2^{n-1} - 3$, we only need to consider the case $L(u^{(n)} + v^{(n)}) < 2^{n-1}$. Thus $Left(u^{(n)} + v^{(n)}) = Right(u^{(n)} + v^{(n)})$ and $W(Left(u^{(n)} + v^{(n)})) = 2$.

By Lemma 2.1.3 in Section 2.1, $L(u^{(n)} + v^{(n)}) = 2^{n-1} - 2^m$, $0 \le m < n-1$.

Thus $L(s^{(n)} + u^{(n)} + v^{(n)}) \ge L(s^{(n)})$, so the 2-error linear complexity of $s^{(n)} + u^{(n)}$ is still c.

2). As $s^{(n)}$ is a binary sequence with linear complexity $c = 2^{n-1} - 2^m, 0 \le m < n-1$, so the 2-error linear complexity of $s^{(n)} + u^{(n)}$ must be less than c when $L(u^{(n)} + v^{(n)}) = c$. □

Lemma 2.2.2 Suppose that $s^{(n)} \ne t^{(n)}$ are two binary sequences with the same linear complexity $c, 1 \le c \le 2^{n-2}$, $u^{(n)} \ne v^{(n)}$ are two binary sequences with $W(u^{(n)}) = 0$ or 2,

and $W(v^{(n)}) = 0$ or 2. Then $s^{(n)} + u^{(n)} \neq t^{(n)} + v^{(n)}$.

Proof. First the following is true.

$$s^{(n)} + u^{(n)} \neq t^{(n)} + v^{(n)} \Leftrightarrow s^{(n)} + u^{(n)} + v^{(n)} \neq t^{(n)} \Leftrightarrow u^{(n)} + v^{(n)} \neq s^{(n)} + t^{(n)}.$$

Note that $s^{(n)}$ and $t^{(n)}$ are two different binary sequences with the same linear complexity $c, 1 \leq c \leq 2^{n-2}$, from Lemma 2.1.2 the linear complexity of $s^{(n)} + t^{(n)}$ is less than 2^{n-2}. By the Games-Chan algorithm (Games and Chan, 1983), one period of $s^{(n)} + t^{(n)}$ can be divided into 4 equal parts.

Suppose that $u^{(n)} + v^{(n)} = s^{(n)} + t^{(n)}$. Then one period of $u^{(n)} + v^{(n)}$ can be divided into 4 equal parts. It follows that the linear complexity of $u^{(n)} + v^{(n)}$ is 2^{n-2}, which contradicts the fact that the linear complexity of $s^{(n)} + t^{(n)}$ is less than 2^{n-2}. □

Next we divide the 2-error linear complexity into three categories and deal with them by Lemma 2.2.3, Lemma 2.2.4 and Lemma 2.2.5, respectively. First we consider the category of $2^{n-1} - 2^{n-m}$.

Lemma 2.2.3 Let $N_2(2^{n-1} - 2^{n-m})$ be the number of 2^n-periodic binary sequences with linear complexity less than 2^n and the 2-error linear complexity $2^{n-1} - 2^{n-m}, n \geq 2, 1 < m \leq n$. Then

$$N_2(2^{n-1} - 2^{n-m}) = (1 + \begin{pmatrix} 2^n \\ 2 \end{pmatrix} - 3 \times 2^{n+m-3}) 2^{2^{n-1}-2^{n-m}-1}.$$

Proof. We first sketch the proof. Let $S = \{s | L(s) = 2^{n-1} - 2^{n-m}\}, E = \{e | W(e) = 0 \text{ or } 2\}, S + E = \{s + e | s \in S, e \in E\}$, where s is a sequence with linear complexity $2^{n-1} - 2^{n-m}$, and e is an error sequence with $W(e) = 0$ or 2. With the sieve method in combinatorics, we attempt to sieve all the sequences $s + e$ with $L_2(s + e) = 2^{n-1} - 2^{n-m}$ in $S + E$.

By Lemma 2.1.6 in Section 2.1, the number of 2^n-periodic binary sequences with linear complexity $2^{n-1} - 2^{n-m}$ is $2^{2^{n-1}-2^{n-m}-1}$. As the number of 2^n-periodic binary sequences in E is $1 + \begin{pmatrix} 2^n \\ 2 \end{pmatrix}$, the number of 2^n-periodic binary sequences $s + e \in S + E$ is at most $(1 + \begin{pmatrix} 2^n \\ 2 \end{pmatrix}) 2^{2^{n-1}-2^{n-m}-1}$.

It remains to characterize two cases. One is that $s+e \in S+E$, but $L_2(s+e) < 2^{n-1}-2^{n-m}$. The other is the case that $s^{(n)}+u^{(n)}, t^{(n)}+v^{(n)} \in S+E$ with $s^{(n)} \neq t^{(n)}$, $u^{(n)} \neq v^{(n)}$, but $s^{(n)}+u^{(n)} = t^{(n)}+v^{(n)}$.

The following is the detailed proof.

To deal with the $s^{(n)}+u^{(n)}$ with $W(u^{(n)})=2$, we need to give the following two facts.

Fact 1. Suppose that

$$u^{(n)}+v^{(n)} = \{\cdots,0,\overbrace{\underbrace{1,0,\cdots,0,1}_{2^{n-m}(2k+1)},0,\cdots,0,1}^{2^{n-1}},0,\cdots,0,1,0,\cdots\}$$

where $Left(u^{(n)}+v^{(n)}) = Right(u^{(n)}+v^{(n)})$ in each period, and the distance of first two 1s is $2^{n-m}(2k+1)$ with k being an integer. Here the distance of two elements is defined as the difference of their indexes. By Lemma 2.1.3 in Section 2.1, $L(u^{(n)}+v^{(n)}) = 2^{n-1}-2^{n-m}$.

Fact 2. Suppose that $u^{(n)}$ is a binary sequence with $W(u^{(n)})=2$, and there exist two nonzero elements whose distance is $2^{n-m}(2k+1)$ or 2^{n-1}, with k being an integer. Then it is easy to find a binary sequence $v^{(n)}$ with $W(v^{(n)})=2$, such that $L(u^{(n)}+v^{(n)}) = 2^{n-1}-2^{n-m}$.

In the case that the distance of two nonzero elements is $2^{n-m}(2k+1)$, $Left(v^{(n)}) = Right(u^{(n)})$, $Right(v^{(n)}) = Left(u^{(n)})$. Thus there exists exactly one binary sequence $v^{(n)}$.

Without loss of generality, one can assume the case that the distance of two nonzero elements is $2^{n-m}(2k+1)$ and

$$u^{(n)} = \{\cdots,0,\overbrace{\underbrace{1,0,\cdots,0,1}_{2^{n-m}(2k+1)},0,\cdots,0,0}^{2^{n-1}},0,\cdots,0,0,0,\cdots\}$$

Then $v^{(n)}$ can be constructed as the following.

$$v^{(n)} = \{\cdots,0,0,0,\cdots,0,\overbrace{0,0,\cdots,0,\underbrace{1,0,\cdots,0,1}_{2^{n-m}(2k+1)}}^{2^{n-1}},0,\cdots\}$$

If one assumes the case that the distance of two nonzero elements is 2^{n-1} and

$$u^{(n)} = \{\cdots, 0, \overbrace{\underbrace{1, 0, \cdots, 0, 0}_{2^{n-m}(2k+1)}, 0, \cdots, 0, 1}^{2^{n-1}}, 0, \cdots, 0, 0, 0, \cdots\}$$

Then $v^{(n)}$ can be constructed as the following.

$$v^{(n)} = \{\cdots, 0, 0, 0, \cdots, 0, \overbrace{1, 0, \cdots, 0, \underbrace{0, 0, \cdots, 0, 1}_{2^{n-m}(2k+1)}}^{2^{n-1}}, 0, \cdots\}$$

Suppose that $s^{(n)}$ is a binary sequence with linear complexity $2^{n-1} - 2^{n-m}$. By Lemma 2.2.1, there exists a binary sequence $u^{(n)}$ with $W(u^{(n)}) = 2$, such that the 2-error linear complexity of $u^{(n)} + s^{(n)}$ is less than $2^{n-1} - 2^{n-m}$.

Now let us divide one period of $u^{(n)}$ into 2^{n-m} subsequences in the following form,

$\{u_a, u_{a+2^{n-m}}, u_{a+2^{n-m+1}}, \cdots, u_{a+(2^m-1)\times 2^{n-m}}\}, 0 \le a < 2^{n-m}$.

If two nonzero elements of $u^{(n)}$ are in the same subsequence, then the number of these $u^{(n)}$ can be given by

$$C1 = 2^{n-m} \times \begin{pmatrix} 2^m \\ 2 \end{pmatrix}.$$

Here 2^{n-m} represents the number of selections when one selects 1 subsequence, and $\begin{pmatrix} 2^m \\ 2 \end{pmatrix}$ represents the number of selections without consideration of the order when one selects two elements in one subsequence.

Suppose that two nonzero elements of $u^{(n)}$ are in the same subsequence, and the distance of the two nonzero elements is $2^{n-m}(2k+1)$ or 2^{n-1}, with k being an integer. From Fact 2, the 2-error linear complexity of $u^{(n)} + s^{(n)}$ will be less than $2^{n-1} - 2^{n-m}$.

Suppose that two nonzero elements of $u^{(n)}$ are in the same subsequence, and the distance of the two nonzero elements is not $2^{n-m}(2k+1)$ with k being an integer. Then the distance of the two nonzero elements must be $2^{n-m+x}(2k+1)$ with k being an integer and x being an positive integer. This is equivalent to the fact that one period of $u^{(n)}$ is divided into 2^{n-m+1} subsequences and two nonzero elements of $u^{(n)}$ are in the same subsequence. Therefore, the number of these $u^{(n)}$ can be given by $2^{n-m+1} \times \begin{pmatrix} 2^{m-1} \\ 2 \end{pmatrix}$.

Of these $u^{(n)}$, there are $2^{n-m+1} \times 2^{m-2} = 2^{n-1}$ sequences, in each sequence the distance of the two nonzero elements is 2^{n-1}.

So, if two nonzero elements of $u^{(n)}$ are in the same subsequence, and the distance of the two nonzero elements is neither $2^{n-m}(2k+1)$ nor 2^{n-1}, then the number of these $u^{(n)}$ can be given by

$$C2 = 2^{n-m+1} \times \left(\begin{array}{c} 2^{m-1} \\ 2 \end{array} \right) - 2^{n-1}.$$

Suppose that two nonzero elements of $u^{(n)}$ are in the same subsequence, and the distance of the two nonzero elements is neither $2^{n-m}(2k+1)$ nor 2^{n-1}. Then the distance of the two nonzero elements must be $2^{n-m+x}(2k+1)$ with k being an integer and x being an positive integer. From Fact 2, there exists exactly one binary sequence $v^{(n)}$ with $W(v^{(n)}) = 2$, such that $L(u^{(n)} + v^{(n)}) = 2^{n-1} - 2^{n-r}, 1 < r = m - x < m$. Let $t^{(n)} = s^{(n)} + u^{(n)} + v^{(n)}$. Then $L(t^{(n)}) = L(s^{(n)}) = 2^{n-1} - 2^{n-m}$ and $s^{(n)} + u^{(n)} = t^{(n)} + v^{(n)}$.

Suppose that two nonzero elements of $u^{(n)}$ are not in the same subsequence. Then the distance of the two nonzero elements must be $2^{n-(m+x)}(2k+1)$ with k being an integer and x being an positive integer. From Fact 1, there does not exist a binary sequence $v^{(n)}$ with $W(v^{(n)}) = 2$, such that $L(u^{(n)} + v^{(n)}) = 2^{n-1} - 2^{n-m}$. This leads to the following,

$$\begin{aligned} & N_2(2^{n-1} - 2^{n-m}) \\ = \; & [1 + \left(\begin{array}{c} 2^n \\ 2 \end{array} \right) - (C1 - C2) - C2/2] 2^{2^{n-1} - 2^{n-m} - 1} \\ = \; & [1 + \left(\begin{array}{c} 2^n \\ 2 \end{array} \right) - 2^{n-m} \left(\begin{array}{c} 2^m \\ 2 \end{array} \right) + 2^{n-m} \left(\begin{array}{c} 2^{m-1} \\ 2 \end{array} \right) - 2^{n-2}] \times 2^{2^{n-1} - 2^{n-m} - 1} \\ = \; & (1 + \left(\begin{array}{c} 2^n \\ 2 \end{array} \right) - 3 \times 2^{n+m-3}) 2^{2^{n-1} - 2^{n-m} - 1}. \end{aligned}$$

□

Next we consider the category of $2^{n-1} - 2^{n-m} + x$.

Lemma 2.2.4 Let $N_2(2^{n-1} - 2^{n-m} + x)$ be the number of 2^n-periodic binary sequences with linear complexity less than 2^n and the 2-error linear complexity $2^{n-1} - 2^{n-m} + x, n >$

$3, 1 < m < n-1, 0 < x < 2^{n-m-1}$. Then

$$\begin{aligned} & N_2(2^{n-1} - 2^{n-m} + x) \\ = \; & [1 + \begin{pmatrix} 2^n \\ 2 \end{pmatrix} + 2^{n-m} - 2^{n+m-2}]2^{2^{n-1}-2^{n-m}+x-1} \end{aligned}$$

Proof. Let $S = \{s|L(s) = 2^{n-1} - 2^{n-m} + x\}, E = \{e|W(e) = 0 \text{ or } 2\}, S + E = \{s + e|s \in S, e \in E\}$. By Lemma 2.1.6 in Section 2.1, the number of 2^n-periodic binary sequences with linear complexity $2^{n-1} - 2^{n-m} + x$ is $2^{2^{n-1}-2^{n-m}+x-1}$. As the number of 2^n-periodic binary sequences in E is $1 + \begin{pmatrix} 2^n \\ 2 \end{pmatrix}$, the number of 2^n-periodic binary sequences $s + e \in S + E$ is at most $(1 + \begin{pmatrix} 2^n \\ 2 \end{pmatrix})2^{2^{n-1}-2^{n-m}+x-1}$.

Suppose that $s^{(n)}$ is a binary sequence with linear complexity $2^{n-1} - 2^{n-m} + x$, and $u^{(n)}$ is a binary sequence with $W(u^{(n)}) = 0$ or 2. By Lemma 2.2.1, the 2-error linear complexity of $u^{(n)} + s^{(n)}$ is $2^{n-1} - 2^{n-m} + x$. It remains to prove the case of $s^{(n)} + u^{(n)}, t^{(n)} + v^{(n)} \in S + E$ with $s^{(n)} \neq t^{(n)}$, $u^{(n)} \neq v^{(n)}$, but $s^{(n)} + u^{(n)} = t^{(n)} + v^{(n)}$.

Suppose that $u^{(n)}$ is a binary sequence with $W(u^{(n)}) = 2$, and there exist two nonzero elements whose distance is $2^{n-r}(1 + 2a), 1 < r \leq m, a \geq 0$. Then there exists one binary sequence $v^{(n)}$ with $W(v^{(n)}) = 2$, such that $L(u^{(n)} + v^{(n)}) = 2^{n-1} - 2^{n-r}$. Here the construction of $v^{(n)}$ is similar to that of Lemma 2.2.3. Let $t^{(n)} = s^{(n)} + u^{(n)} + v^{(n)}$. Then $L(t^{(n)}) = L(s^{(n)}) = 2^{n-1} - 2^{n-m} + x$ and $s^{(n)} + u^{(n)} = t^{(n)} + v^{(n)}$.

Now let us divide one period of $u^{(n)}$ into 2^{n-m} subsequences in the following form,

$$\{u_a, u_{a+2^{n-m}}, u_{a+2^{n-m+1}}, \cdots, u_{a+(2^m-1)\times 2^{n-m}}\}, 0 \leq a < 2^{n-m}.$$

If two nonzero elements of $u^{(n)}$ are in the same subsequence, and their distance is 2^{n-1}, then there exist $2^{m-1} - 1$ binary sequences $v^{(n)}$ with $W(v^{(n)}) = 2$, such that $L(u^{(n)} + v^{(n)}) = 2^{n-1} - 2^{n-r}, 1 < r \leq m$. Let $t^{(n)} = s^{(n)} + u^{(n)} + v^{(n)}$. Then $s^{(n)} + u^{(n)} = t^{(n)} + v^{(n)}$. The number of these $u^{(n)}$ can be given by $D1 = 2^{n-m} \times 2^{m-1} = 2^{n-1}$.

Suppose that two nonzero elements of $u^{(n)}$ are in the same subsequence, and their distance is $2^{n-r}(1 + 2a), 1 < r \leq m, a \geq 0$. Here $2^{n-r}(1 + 2a) < 2^{n-1}$. Then there exists one binary sequence $v^{(n)}$, with $W(v^{(n)}) = 2$, such that $L(u^{(n)} + v^{(n)}) = 2^{n-1} - 2^{n-r}$. The number of

these $u^{(n)}$ can be given by

$$D2 = 2^{n-m}[\begin{pmatrix} 2^m \\ 2 \end{pmatrix} - 2^{m-1}].$$

This will lead to the following,

$$\begin{aligned}
& N_2(2^{n-1} - 2^{n-m} + x) \\
= \; & [1 + \begin{pmatrix} 2^n \\ 2 \end{pmatrix} - \frac{2^{m-1}-1}{2^{m-1}} \times D1 - \frac{1}{2} \times D2]2^{2^{n-1}-2^{n-m}+x-1} \\
= \; & \{1 + \begin{pmatrix} 2^n \\ 2 \end{pmatrix} - \frac{2^{m-1}-1}{2^{m-1}} \times 2^{n-1} - 2^{n-m-1}[\begin{pmatrix} 2^m \\ 2 \end{pmatrix} - 2^{m-1}]\}2^{2^{n-1}-2^{n-m}+x-1} \\
= \; & \{1 + \begin{pmatrix} 2^n \\ 2 \end{pmatrix} - (2^{m-1}-1) \times 2^{n-m} - 2^{n-m-1}[\begin{pmatrix} 2^m \\ 2 \end{pmatrix} - 2^{m-1}]\}2^{2^{n-1}-2^{n-m}+x-1} \\
= \; & [1 + \begin{pmatrix} 2^n \\ 2 \end{pmatrix} + 2^{n-m} - 2^{n+m-2}]2^{2^{n-1}-2^{n-m}+x-1}
\end{aligned}$$

□

Finally we would consider the category for $1 \leq c \leq 2^{r-2} - 1$.

Lemma 2.2.5 Let $L(r,c) = 2^n - 2^r + c, 3 \leq r \leq n, 1 \leq c \leq 2^{r-2} - 1$, and $N_2(L(r,c))$ be the number of 2^n-periodic binary sequences with linear complexity less than 2^n and the 2-error linear complexity $L(r,c)$. Then

$$N_2(L) = \begin{cases} 1 + \begin{pmatrix} 2^n \\ 2 \end{pmatrix}, & L = 0 \\ 2^{L-1}(1 + \begin{pmatrix} 2^r \\ 2 \end{pmatrix}), & L = L(r,c) \end{cases}$$

Proof. Suppose that s is a binary sequence with first period $s^{(n)} = \{s_0, s_1, s_2, \cdots, s_{2^n-1}\}$, and $L(s) = L(r,c) = 2^n - 2^r + c, 3 \leq r \leq n, 1 \leq c \leq 2^{r-2} - 1$. By the Games-Chan algorithm (Games and Chan, 1983), $Left(s^{(t)}) \neq Right(s^{(t)}), r+1 \leq t \leq n$, where $s^{(t)} = \varphi_{t+1} \cdots \varphi_n(s^{(n)})$.

First we consider the case of $W(s^{(n)}) = 0$. There is only one binary sequence of this kind.

Let us consider the case of $W(s^{(n)}) = 2$. There are two nonzero bits in $\{s_0, s_1, \cdots, s_{2^n-1}\}$, thus there are $\begin{pmatrix} 2^n \\ 2 \end{pmatrix}$ binary sequences of this kind.

So $N_2(0) = 1 + \begin{pmatrix} 2^n \\ 2 \end{pmatrix}$.

It is our turn to consider the case of $L(r,c) = 2^n - 2^r + c$, $3 \le r \le n, 1 \le c \le 2^{r-2} - 1$. Suppose that $s^{(n)}$ is a binary sequence with $L(s^{(n)}) = L(r,c)$. Note that $L(r,c) = 2^n - 2^r + c = 2^{n-1} + \cdots + 2^r + c$. By the Games-Chan algorithm, $Left(s^{(r)}) = Right(s^{(r)})$, and $L(s^{(r)}) = c$.

It is known that the number of binary sequences $t^{(r)}$ with $W(t^{(r)}) = 0$ or 2 is $1 + \begin{pmatrix} 2^r \\ 2 \end{pmatrix}$.

By Lemma 2.2.1, the 2-error linear complexity of $s^{(r)} + t^{(r)}$ is c.

By Lemma 2.1.6 in Section 2.1 and Lemma 2.2.2, the number of binary sequences $s^{(r)} + t^{(r)}$ is $2^{c-1} \times (1 + \begin{pmatrix} 2^r \\ 2 \end{pmatrix})$

By Lemma 2.1.5 in Section 2.1, $\varphi_{t+1}^{-1}(s^{(t)}) = \{v \in F_2^{2^{t+1}} | \varphi_{t+1}(v) = s^{(t)}\}$, which is the preimage of $s^{(t)}$ with cardinality 2^{2^t}, where $r \le t < n$. Thus there are $2^{2^{n-1}+\cdots+2^r} = 2^{2^n - 2^r}$ binary sequences $s^{(n)} + t^{(n)}$, such that $s^{(r)} + t^{(r)} = \varphi_{r+1} \cdots \varphi_n(s^{(n)} + t^{(n)})$, $t^{(r)} = \varphi_{r+1} \cdots \varphi_n(t^{(n)})$ and $W(t^{(n)}) = W(t^{(r)})$.

Thus the 2-error linear complexity of $s^{(n)} + t^{(n)}$ is

$$2^{n-1} + \cdots + 2^r + L_2(s^{(r)} + t^{(r)}) = 2^n - 2^r + c = L(r,c).$$

Therefore, $N_2(L(r,c)) = 2^{2^n - 2^r} \times 2^{c-1} \times (1 + \begin{pmatrix} 2^r \\ 2 \end{pmatrix}) = 2^{L(r,c)-1}(1 + \begin{pmatrix} 2^r \\ 2 \end{pmatrix})$ □

Based on the results above, we can have the proof of Theorem 2.2.1 now.

Proof. By Lemma 2.2.5, we now only need to consider the case of $3 \le r \le n, 2^{r-2} \le c \le 2^{r-1} - 1$.

By Lemma 2.1.6 in Section 2.1 and Lemma 2.2.3,

$$N_2(L(r,c)) = 2^{L(r,c)-1}(\begin{pmatrix} 2^r \\ 2 \end{pmatrix} + 1 - 3 \times 2^{r+m-3})$$

for $3 \le r \le n, c = 2^{r-1} - 2^{r-m}, 1 < m \le r$.

By Lemma 2.1.6 in Section 2.1 and Lemma 2.2.4,

$$N_2(L(r,c)) = 2^{L(r,c)-1}(\begin{pmatrix} 2^r \\ 2 \end{pmatrix} + 1 + 2^{r-m} - 2^{r+m-2})$$

for $4 \leq r \leq n, c = 2^{r-1} - 2^{r-m} + x, 1 < m < r-1, 0 < x < 2^{r-m-1}$.

This completes the proof. □

Notice that for a 2^n-periodic binary sequence with linear complexity less than 2^n, the change of three bits in each period results in a sequence with odd number of nonzero bits in each period, which will have linear complexity 2^n again. So from Theorem 2.2.1, we have also obtained the counting functions for the 3-error linear complexity for 2^n-periodic binary sequences with linear complexity less than 2^n.

2.3 Counting functions for the 3-error linear complexity

For a 2^n-periodic binary sequence with linear complexity 2^n, the change of two bits in each period results in a sequence with odd number of nonzero bits in the same period, which has linear complexity 2^n. In this section, we thus focus on the 3-error linear complexity.

The main result of this section is the following theorem.

Theorem 2.3.1 Let $L(r,c) = 2^n - 2^r + c$, or $2^n - 2^3 + 1$, $4 \leq r \leq n, 1 \leq c \leq 2^{r-1} - 1$, and $N_3(L(r,c))$ be the number of 2^n-periodic binary sequences with linear complexity 2^n

and the 3-error linear complexity $L(r,c)$. Let

$$\begin{aligned} & f(n,m) \\ = & \binom{2^n}{3} - 2^{n-m}\binom{2^m}{3} - \binom{2^{n-m}}{2}\binom{2^m}{2}2^{m+1} \\ & + \binom{2^{n-m}}{2} \times 2^{2m}(2^{m-2}-1) + 2^{n-m-1} \times \binom{2^{m-1}}{3} \\ & -2^{n-2} \times (2^{m-2}-1) \end{aligned}$$

$$\begin{aligned} & g(n,m) \\ = & \binom{2^n}{3} - (2^{m-2}-1) \times 2^{n+1} \\ & -(2^{m-1}-1) \times \binom{2^{n-m}}{2} \times 2^{m+1} \\ & -3 \times 2^{n-m-2}[\binom{2^m}{3} - 4\binom{2^{m-1}}{2}] \\ & -\binom{2^{n-m}}{2} \times [\binom{2^m}{2} - 2^{m-1}] \times 2^m \end{aligned}$$

Then

$$N_3(L) = \begin{cases} \binom{2^n}{3} + 2^n, \quad L = 0 \\ 2^{L(r,c)-1}(\binom{2^r}{3} + 2^r), \\ \qquad L = L(r,c), 1 \le c \le 2^{r-2}-1, r > 2 \\ 2^{L(r,c)-1} f(r,m), \\ \qquad L = L(r,c), c = 2^{r-1} - 2^{r-m}, 1 < m \le r, r > 3 \\ 2^{L(r,c)-1} g(r,m), \\ \qquad L = L(r,c), c = 2^{r-1} - 2^{r-m} + x, \\ \qquad 1 < m < r-1, 0 < x < 2^{r-m-1}, r > 3 \\ 0, \qquad\qquad\qquad \text{otherwise} \end{cases}$$

To prove Theorem 2.3.1, we need to give several lemmas.

With the idea similar to that used in previous section, we first investigate the sequence

$s^{(n)} + u^{(n)}$.

Lemma 2.3.1 1). Suppose $s^{(n)}$ is a binary sequence with linear complexity $c, 1 \leq c \leq 2^{n-1} - 3$, $c \neq 2^{n-1} - 2^m, 2 \leq m < n-1$, $u^{(n)}$ is a binary sequence with linear complexity 2^n, and $W(u^{(n)}) = 1$ or 3. Then the 3-error linear complexity of $s^{(n)} + u^{(n)}$ is also c.

2). If $s^{(n)}$ is a binary sequence with linear complexity $c = 2^{n-1} - 2^m, 0 \leq m < n-1$, then there exists a binary sequence $u^{(n)}$ with linear complexity 2^n, such that the 3-error linear complexity of $s^{(n)} + u^{(n)}$ is less than c.

Proof. Note that the 3-error linear complexity of $s^{(n)}$ is the smallest linear complexity that can be obtained when any $u^{(n)}$ with $W(u^{(n)}) = 1$ or 3 is added to $s^{(n)}$.

Suppose that $v^{(n)}$ is a binary sequence, $v^{(n)} \neq u^{(n)}$, and $W(v^{(n)}) = 1$ or 3.

1). As $c \leq 2^{n-1} - 3$, we only need to consider the case of $L(u^{(n)} + v^{(n)}) < 2^{n-1}$. In this case, $Left(u^{(n)} + v^{(n)}) = Right(u^{(n)} + v^{(n)})$ and $W(Left(u^{(n)} + v^{(n)})) = 2$.

By Lemma 2.1.3, $L(u^{(n)} + v^{(n)}) = 2^{n-1} - 2^m$, $0 \leq m < n-1$.

Thus $L(s^{(n)} + u^{(n)} + v^{(n)}) \geq L(s^{(n)})$, so the 3-error linear complexity of $s^{(n)} + u^{(n)}$ is c.

2). As $s^{(n)}$ is a binary sequence with linear complexity $c = 2^{n-1} - 2^m, 0 \leq m < n-1$. So the 3-error linear complexity of $s^{(n)} + u^{(n)}$ must be less than c when $L(u^{(n)} + v^{(n)}) = c$. $\square$

Lemma 2.3.2 Suppose that $s^{(n)} \neq t^{(n)}$ are two binary sequences with the same linear complexity $c, 1 \leq c \leq 2^{n-2}$, $u^{(n)} \neq v^{(n)}$ are two binary sequences with linear complexity 2^n as well as $W(u^{(n)}) = 1$ or 3, $W(v^{(n)}) = 1$ or 3. Then $s^{(n)} + u^{(n)} \neq t^{(n)} + v^{(n)}$.

Proof. First the following is true.

$$s^{(n)} + u^{(n)} \neq t^{(n)} + v^{(n)} \Leftrightarrow s^{(n)} + u^{(n)} + v^{(n)} \neq t^{(n)} \Leftrightarrow u^{(n)} + v^{(n)} \neq s^{(n)} + t^{(n)}$$

Note that $s^{(n)}$ and $t^{(n)}$ are two different binary sequences with linear complexity $c, 1 \leq c \leq 2^{n-2}$, so the linear complexity of $s^{(n)} + t^{(n)}$ is less than 2^{n-2}, and one period of $s^{(n)} + t^{(n)}$ can be divided into 4 equal parts.

Suppose that $u^{(n)} + v^{(n)} = s^{(n)} + t^{(n)}$. Then one period of $u^{(n)} + v^{(n)}$ can be divided into 4 equal parts, thus $W(u^{(n)} + v^{(n)}) = 4$. It follows that the linear complexity of $u^{(n)} + v^{(n)}$ is 2^{n-2}, which contradicts the fact that the linear complexity of $s^{(n)} + t^{(n)}$ is less than 2^{n-2}. □

Next, we divide the 3-error linear complexity into three categories and deal with them by Lemma 2.3.3, Lemma 2.3.4 and Lemma 2.3.5, respectively. First consider the category of $2^{n-1} - 2^{n-m}$.

Lemma 2.3.3 Let $N_3(2^{n-1} - 2^{n-m})$ be the number of 2^n-periodic binary sequences with linear complexity 2^n and the 3-error linear complexity $2^{n-1} - 2^{n-m}, n > 3, 1 < m \leq n$. Then

$$\begin{aligned} & N_3(2^{n-1} - 2^{n-m}) \\ = \; & [\binom{2^n}{3} - 2^{n-m}\binom{2^m}{2} - \binom{2^{n-m}}{2}\binom{2^m}{2}2^{m+1} \\ & + \binom{2^{n-m}}{2} \times 2^{2m}(2^{m-2} - 1) + 2^{n-m-1} \times \binom{2^{m-1}}{3} \\ & - 2^{n-2} \times (2^{m-2} - 1)]2^{2^{n-1}-2^{n-m}-1} \end{aligned}$$

Proof. Let $S = \{s|L(s) = 2^{n-1} - 2^{n-m}\}, E = \{e|W(e) = 1 \text{ or } 3\}, S + E = \{s + e|s \in S, e \in E\}$. By Lemma 2.1.6 in Section 2.1, the number of 2^n-periodic binary sequences with linear complexity $2^{n-1} - 2^{n-m}$ is $2^{2^{n-1}-2^{n-m}-1}$. As the number of 2^n-periodic binary sequences in E is $2^n + \binom{2^n}{3}$, the number of 2^n-periodic binary sequences $s + e \in S + E$ is at most $(2^n + \binom{2^n}{3})2^{2^{n-1}-2^{n-m}-1}$.

It remains to prove the following two cases. One is that $s + e \in S + E$, but $L_3(s + e) < 2^{n-1} - 2^{n-m}$. The other is the case that $s^{(n)} + u^{(n)}, t^{(n)} + v^{(n)} \in S + E$ with $s^{(n)} \neq t^{(n)}$, $u^{(n)} \neq v^{(n)}$, but $s^{(n)} + u^{(n)} = t^{(n)} + v^{(n)}$.

Suppose that $s^{(n)}$ is a binary sequence with linear complexity $2^{n-1} - 2^{n-m}$, and $u^{(n)}$ is a binary sequence with $W(u^{(n)}) = 1$. One can construct a binary sequence $v^{(n)}$ with $W(v^{(n)}) = 3$, such that $L(u^{(n)} + v^{(n)}) = 2^{n-1} - 2^{n-m}$. So the 3-error linear complexity of $u^{(n)} + s^{(n)}$ is less than $2^{n-1} - 2^{n-m}$.

To deal with the $s^{(n)} + u^{(n)}$ with $W(u^{(n)}) = 3$, the following fact is used.

Suppose that $u^{(n)}$ is a binary sequence with $W(u^{(n)}) = 3$, and there exist two nonzero elements whose distance is $2^{n-r}(1 + 2a), 1 < r \leq m, a \geq 0$ or 2^{n-1}. Then one can find 1 binary sequence $v^{(n)}$ with $W(v^{(n)}) = 3$, such that $L(u^{(n)} + v^{(n)}) = 2^{n-1} - 2^{n-r}$ with $W(u^{(n)} + v^{(n)}) = 4$. If $r = m$, then $L(u^{(n)} + v^{(n)}) = 2^{n-1} - 2^{n-m}$, hence the 3-error linear complexity of $u^{(n)} + s^{(n)}$ is less than $2^{n-1} - 2^{n-m}$.

Without loss of generality, assume that $supp(u^{(n)}) = \{y1, y2, y3\}$, and the distance of $y1$ and $y2$ is $2^{n-r}(1+2a), 1 < r \leq m, a \geq 0$. Then the construction of $v^{(n)}$ with $supp(v^{(n)}) = \{z1, z2, y3\}$ is similar to that of Lemma 2.2.3. Here $u^{(n)}$ and $v^{(n)}$ have exactly one common nonzero element, so that $W(u^{(n)} + v^{(n)}) = 4$.

Let us divide one period of $u^{(n)}$ into 2^{n-m} subsequences with the following form

$$\{u_a, u_{a+2^{n-m}}, u_{a+2^{n-m+1}}, \cdots, u_{a+(2^m-1)\times 2^{n-m}}\}, 0 \leq a < 2^{n-m}.$$

If only two nonzero elements of $u^{(n)}$ are in the same subsequence, then the number of these $u^{(n)}$ can be given by $E1 = 2\begin{pmatrix} 2^{n-m} \\ 2 \end{pmatrix} \times \begin{pmatrix} 2^m \\ 2 \end{pmatrix} \times 2^m$. Here $2\begin{pmatrix} 2^{n-m} \\ 2 \end{pmatrix}$ represents the number of permutations when one selects 2 subsequences, $\begin{pmatrix} 2^m \\ 2 \end{pmatrix}$ represents the number of selections without consideration of the order when one selects 2 elements in one subsequence and 2^m represents the number of selections when one selects 1 element in another subsequence.

Suppose that only two nonzero elements of $u^{(n)}$ are in the same subsequence, and the distance of the two nonzero elements is not $2^{n-m}(2k+1)$. Then the number of these $u^{(n)}$ can be given by $2\begin{pmatrix} 2^{n-m} \\ 2 \end{pmatrix} \times 2 \times \begin{pmatrix} 2^{m-1} \\ 2 \end{pmatrix} \times 2^m$. Of these $u^{(n)}$, there are $2\begin{pmatrix} 2^{n-m} \\ 2 \end{pmatrix} \times 2^{m-1} \times 2^m$ sequences, in which the distance of the two nonzero elements is 2^{n-1}.

So, if only two nonzero elements of $u^{(n)}$ are in the same subsequence, and the distance of the two nonzero elements is neither $2^{n-m}(2k+1)$ nor 2^{n-1}, then the number of these $u^{(n)}$ can be given by

$$
\begin{aligned}
E2 &= 2\begin{pmatrix} 2^{n-m} \\ 2 \end{pmatrix} \times 2 \times \begin{pmatrix} 2^{m-1} \\ 2 \end{pmatrix} \times 2^m - 2\begin{pmatrix} 2^{n-m} \\ 2 \end{pmatrix} \times 2^{m-1} \times 2^m \\
&= \begin{pmatrix} 2^{n-m} \\ 2 \end{pmatrix} \times 2^{2m} \times (2^{m-1} - 2).
\end{aligned}
$$

Suppose that $u^{(n)}$ is a binary sequence with $W(u^{(n)}) = 3$, and there exist two nonzero elements whose distance is a multiple of 2^{n-m+1}, but is not 2^{n-1}. Thus we can assume the distance of two nonzero elements is $2^{n-r}(1+2a), 1 < r < m, a \geq 0$, hence there exists one binary sequence $v^{(n)}$ with $W(v^{(n)}) = 3$, such that $L(u^{(n)}+v^{(n)}) = 2^{n-1}-2^{n-r}, 1 < r < m$. Let $t^{(n)} = s^{(n)} + u^{(n)} + v^{(n)}$. Then $L(t^{(n)}) = L(s^{(n)}) = 2^{n-1} - 2^{n-m}$ and $s^{(n)} + u^{(n)} = t^{(n)} + v^{(n)}$, where there exist exactly two nonzero elements in $v^{(n)}$ whose distance is a multiple of 2^{n-m+1}.

If all 3 nonzero elements of $u^{(n)}$ are in the same subsequence, then the number of these $u^{(n)}$ can be given by $E3 = 2^{n-m} \times \begin{pmatrix} 2^m \\ 3 \end{pmatrix}$.

Suppose that all 3 nonzero elements of $u^{(n)}$ are in the same subsequence, and there do not exist two nonzero elements whose distance is $2^{n-m}(2k+1)$. Then the number of these $u^{(n)}$ can be given by $2^{n-m+1} \times \begin{pmatrix} 2^{m-1} \\ 3 \end{pmatrix}$. Of these $u^{(n)}$, there are $2^{n-m+1} \times 2^{m-2} \times (2^{m-1}-2) = 2^n \times (2^{m-2}-1)$ sequences, in which there exist two nonzero elements with distance 2^{n-1}.

So, if all 3 nonzero elements of $u^{(n)}$ are in the same subsequence, and there do not exist two nonzero elements whose distance is $2^{n-m}(2k+1)$ or 2^{n-1}, then the number of these $u^{(n)}$ can be given by

$$
E4 = 2^{n-m+1} \times \begin{pmatrix} 2^{m-1} \\ 3 \end{pmatrix} - 2^n \times (2^{m-2} - 1)
$$

Suppose that $u^{(n)}$ is a binary sequence with linear complexity 2^n and all 3 nonzero elements of $u^{(n)}$ are in the same subsequence, and there do not exist two nonzero elements whose distance is $2^{n-m}(2k+1)$ or 2^{n-1}. Thus we can assume that $supp(u^{(n)}) = \{y1, y2, y3\}$, and the distance of $y1$ and $y2$ is $2^{n-r_1}(1+2a_1), 1 < r_1 < m, a_1 \geq 0$, the distance of $y1$ and $y3$ is $2^{n-r_2}(1+2a_2), 1 < r_2 < m, a_2 \geq 0$, the distance of $y2$ and $y3$ is $2^{n-r_3}(1+2a_3), 1 < r_3 < m, a_3 \geq 0$. Similar to that of Lemma 2.2.3, one can construct 3 distinct binary sequences $v_i^{(n)}, 1 \leq i \leq 3$, with linear complexity 2^n and $W(v_i^{(n)}) = 3$, such that $L(u^{(n)} + v_i^{(n)}) =$

$2^{n-1}-2^{n-r_i}, 1 < r_i < m$. Let $t_i^{(n)} = s^{(n)}+u^{(n)}+v_i^{(n)}$. Then $L(t_i^{(n)}) = L(s^{(n)}) = 2^{n-1}-2^{n-m}$ and $s^{(n)} + u^{(n)} = t_i^{(n)} + v_i^{(n)}$.

Here $u^{(n)}$ and $v_i^{(n)}$ have exactly one common nonzero element, so that $W(u^{(n)} + v_i^{(n)}) = 4$. Specifically, $y3 \in supp(v_1^{(n)}), y2 \in supp(v_2^{(n)})$ and $y1 \in supp(v_3^{(n)})$. It follows that,

$$
\begin{aligned}
& N_3(2^{n-1} - 2^{n-m}) \\
= \; & [\binom{2^n}{3} - (E1 - E2) - E2/2 - (E3 - E4) - \frac{3}{4}E4]2^{2^{n-1}-2^{n-m}-1} \\
= \; & [\binom{2^n}{3} - E3 - E1 + E2/2 + E4/4]2^{2^{n-1}-2^{n-m}-1} \\
= \; & [\binom{2^n}{3} - 2^{n-m}\binom{2^m}{3} - \binom{2^{n-m}}{2}\binom{2^m}{2}2^{m+1} \\
& + \binom{2^{n-m}}{2} \times 2^{2m}(2^{m-2} - 1) + 2^{n-m-1} \times \binom{2^{m-1}}{3} \\
& -2^{n-2} \times (2^{m-2} - 1)]2^{2^{n-1}-2^{n-m}-1}.
\end{aligned}
$$

□

Next we consider the category of $2^{n-1} - 2^{n-m} + x$.

Lemma 2.3.4 Let $N_3(2^{n-1} - 2^{n-m} + x)$ be the number of 2^n-periodic binary sequences with linear complexity 2^n and the 3-error linear complexity of $2^{n-1} - 2^{n-m} + x$, where $n > 3, 1 < m < n - 1, 0 < x < 2^{n-m-1}$. Then

$$
\begin{aligned}
& N_3(2^{n-1} - 2^{n-m} + x) \\
= \; & \{\binom{2^n}{3} - (2^{m-2} - 1) \times 2^{n+1} - (2^{m-1} - 1) \times \binom{2^{n-m}}{2} \times 2^{m+1} \\
& -3 \times 2^{n-m-2}[\binom{2^m}{3} - 4\binom{2^{m-1}}{2}] \\
& - \binom{2^{n-m}}{2} \times [\binom{2^m}{2} - 2^{m-1}] \times 2^m\}2^{2^{n-1}-2^{n-m}+x-1}
\end{aligned}
$$

Proof. Let $S = \{s|L(s) = 2^{n-1} - 2^{n-m} + x\}, E = \{e|W(e) = 1 \text{ or } 3\}, S + E = \{s + e|s \in S, e \in E\}$. By Lemma 2.1.6 in Section 2.1, the number of 2^n-periodic binary sequences with

linear complexity $2^{n-1}-2^{n-m}+x$ is $2^{2^{n-1}-2^{n-m}+x-1}$. As the number of 2^n-periodic binary sequences in E is $2^n+\begin{pmatrix} 2^n \\ 3 \end{pmatrix}$, the number of 2^n-periodic binary sequences $s+e \in S+E$ is at most $(2^n+\begin{pmatrix} 2^n \\ 3 \end{pmatrix})2^{2^{n-1}-2^{n-m}+x-1}$.

Suppose that $s^{(n)}$ is a binary sequence with linear complexity $2^{n-1}-2^{n-m}+x$, and $u^{(n)}$ is a binary sequence with $W(u^{(n)})=1$ or 3. By Lemma 2.3.1, the 3-error linear complexity of $u^{(n)}+s^{(n)}$ is $2^{n-1}-2^{n-m}+x$. It remains to prove the case of $s^{(n)}+u^{(n)}, t^{(n)}+v^{(n)} \in S+E$ with $s^{(n)} \neq t^{(n)}$, $u^{(n)} \neq v^{(n)}$, but $s^{(n)}+u^{(n)}=t^{(n)}+v^{(n)}$.

Suppose that $u^{(n)}$ is a binary sequence with $W(u^{(n)})=1$. One can show the following facts.

There is 1 binary sequence $v^{(n)}$ with $W(v^{(n)})=3$, such that $L(u^{(n)}+v^{(n)})=2^{n-1}-2^{n-2}$ and there exist two nonzero elements in $v^{(n)}$ whose distance is 2^{n-2};

There are 2 binary sequences $v^{(n)}$ with $W(v^{(n)})=3$, such that $L(u^{(n)}+v^{(n)})=2^{n-1}-2^{n-3}$ and there exist two nonzero elements in $v^{(n)}$ whose distance is 2^{n-3} or $3\times 2^{n-3}$;

.....

There are 2^{m-2} binary sequences $v^{(n)}$ with $W(v^{(n)})=3$, such that $L(u^{(n)}+v^{(n)})=2^{n-1}-2^{n-m}$ and there exist two nonzero elements in $v^{(n)}$ whose distance is 2^{n-m} or $3\times 2^{n-m}$ or $\cdots$ or $(\frac{2^{n-1}}{2^{n-m}}-1)\times 2^{n-m}$;

Let $t^{(n)}=s^{(n)}+u^{(n)}+v^{(n)}$. Then $L(t^{(n)})=L(s^{(n)})=2^{n-1}-2^{n-m}+x$ and $s^{(n)}+u^{(n)}=t^{(n)}+v^{(n)}$. Note that there are total $1+2+\cdots+2^{m-2}=2^{m-1}-1$ such $t^{(n)}$ and $v^{(n)}$ with $W(v^{(n)})=3$. Thus it is unnecessary to consider the case of $s^{(n)}+u^{(n)}$ with $W(u^{(n)})=1$.

To deal with the $s^{(n)}+u^{(n)}$ with $W(u^{(n)})=3$, the following fact is used.

Suppose that $u^{(n)}$ is a binary sequence with $W(u^{(n)})=3$, and there exist two nonzero elements whose distance is $2^{n-r}(1+2a), 1<r\leq m, a\geq 0$. Then there exists one binary sequence $v^{(n)}$ with $W(v^{(n)})=3$, such that $L(u^{(n)}+v^{(n)})=2^{n-1}-2^{n-r}$ with $W(u^{(n)}+v^{(n)})=4$. Let $t^{(n)}=s^{(n)}+u^{(n)}+v^{(n)}$. Then $L(t^{(n)})=L(s^{(n)})=2^{n-1}-2^{n-m}+x$ and $s^{(n)}+u^{(n)}=t^{(n)}+v^{(n)}$.

Without loss of generality, assume that $supp(u^{(n)})=\{y1,y2,y3\}$, and the distance of $y1$

and $y2$ is $2^{n-r}(1+2a), 1 < r \leq m, a \geq 0$. Then the construction of $v^{(n)}$ with $supp(v^{(n)}) = \{z1, z2, y3\}$ is similar to that of Lemma 2.2.3. Here $u^{(n)}$ and $v^{(n)}$ have one common nonzero element, so that $W(u^{(n)} + v^{(n)}) = 4$.

Let us divide one period of $u^{(n)}$ into 2^{n-m} subsequences with the following form

$$\{u_a, u_{a+2^{n-m}}, u_{a+2^{n-m+1}}, \cdots, u_{a+(2^m-1)\times 2^{n-m}}\}, 0 \leq a < 2^{n-m}.$$

We divide the $s^{(n)} + u^{(n)}$ with $W(u^{(n)}) = 3$ into 4 cases.

Case 1. If all 3 nonzero elements of $u^{(n)}$ are in the same subsequence, and there exist two nonzero elements with distance 2^{n-1}, then there exist $2^{m-1} - 2$ binary sequences $v^{(n)}$ with $W(v^{(n)}) = 3$, such that $L(u^{(n)}+v^{(n)}) = 2^{n-1}-2^{n-r}, 1 < r \leq m$. Let $t^{(n)} = s^{(n)}+u^{(n)}+v^{(n)}$. Then $s^{(n)} + u^{(n)} = t^{(n)} + v^{(n)}$. The number of these $u^{(n)}$ can be given by

$$F1 = 2^{n-m} \times 2 \times \begin{pmatrix} 2^{m-1} \\ 2 \end{pmatrix} \times 2.$$

Case 2. Suppose that $u^{(n)}$ is a binary sequence with linear complexity 2^n and all 3 nonzero elements of $u^{(n)}$ are in the same subsequence, and there do not exist two nonzero elements whose distance is 2^{n-1}. Then there exist 3 distinct binary sequences $v_i^{(n)}, 1 \leq i \leq 3$, with $W(v_i^{(n)}) = 3$, such that $L(u^{(n)}+v_i^{(n)}) = 2^{n-1}-2^{n-r}, 1 < r \leq m$. Let $t_i^{(n)} = s^{(n)}+u^{(n)}+v_i^{(n)}$. Then $s^{(n)} + u^{(n)} = t_i^{(n)} + v_i^{(n)}$. The number of these $u^{(n)}$ can be given by

$$F2 = 2^{n-m}[\begin{pmatrix} 2^m \\ 3 \end{pmatrix} - 2 \times \begin{pmatrix} 2^{m-1} \\ 2 \end{pmatrix} \times 2].$$

Case 3. If only two nonzero elements of $u^{(n)}$ are in the same subsequence, and the distance of the two nonzero elements is 2^{n-1}, then there exist $2^{m-1} - 1$ binary sequences $v^{(n)}$ with $W(v^{(n)}) = 3$, such that $L(u^{(n)}+v^{(n)}) = 2^{n-1}-2^{n-r}, 1 < r \leq m$. Let $t^{(n)} = s^{(n)}+u^{(n)}+v^{(n)}$. Then $s^{(n)} + u^{(n)} = t^{(n)} + v^{(n)}$. The number of these $u^{(n)}$ can be given by

$$F3 = 2 \begin{pmatrix} 2^{n-m} \\ 2 \end{pmatrix} \times 2^{m-1} \times 2^m = \begin{pmatrix} 2^{n-m} \\ 2 \end{pmatrix} \times 2^{2m}.$$

Case 4. If only two nonzero elements of $u^{(n)}$ are in the same subsequence, and the distance of the two nonzero elements is not 2^{n-1}, then there exists one binary sequence $v^{(n)}$ with $W(v^{(n)}) = 3$, such that $L(u^{(n)}+v^{(n)}) = 2^{n-1}-2^{n-r}, 1 < r \leq m$. Let $t^{(n)} = s^{(n)}+u^{(n)}+v^{(n)}$.

Then $s^{(n)} + u^{(n)} = t^{(n)} + v^{(n)}$. The number of these $u^{(n)}$ can be given by

$$F4 = 2\begin{pmatrix} 2^{n-m} \\ 2 \end{pmatrix} \times [\begin{pmatrix} 2^m \\ 2 \end{pmatrix} - 2^{m-1}] \times 2^m.$$

The above calculations will lead to the following,

$$\begin{aligned}
& N_3(2^{n-1} - 2^{n-m} + x) \\
= \; & [\begin{pmatrix} 2^n \\ 3 \end{pmatrix} - \frac{2^{m-1}-2}{2^{m-1}-1} \times F1 - \frac{2^{m-1}-1}{2^{m-1}} \times F3 - \frac{3}{4} \times F2 - \frac{1}{2} \times F4]2^{2^{n-1}-2^{n-m}+x-1} \\
= \; & \{\begin{pmatrix} 2^n \\ 3 \end{pmatrix} - \frac{2^{m-1}-2}{2^{m-1}-1} \times 2^{n-m+2}\begin{pmatrix} 2^{m-1} \\ 2 \end{pmatrix} \\
& -\frac{2^{m-1}-1}{2^{m-1}} \times \begin{pmatrix} 2^{n-m} \\ 2 \end{pmatrix} \times 2^{2m} - \frac{3}{4} \times 2^{n-m}[\begin{pmatrix} 2^m \\ 3 \end{pmatrix} - 4\begin{pmatrix} 2^{m-1} \\ 2 \end{pmatrix}] \\
& -\frac{1}{2} \times 2\begin{pmatrix} 2^{n-m} \\ 2 \end{pmatrix} \times [\begin{pmatrix} 2^m \\ 2 \end{pmatrix} - 2^{m-1}] \times 2^m\}2^{2^{n-1}-2^{n-m}+x-1} \\
= \; & \{\begin{pmatrix} 2^n \\ 3 \end{pmatrix} - (2^{m-2}-1) \times 2^{n+1} - (2^{m-1}-1) \times \begin{pmatrix} 2^{n-m} \\ 2 \end{pmatrix} \times 2^{m+1} \\
& -3 \times 2^{n-m-2}[\begin{pmatrix} 2^m \\ 3 \end{pmatrix} - 4\begin{pmatrix} 2^{m-1} \\ 2 \end{pmatrix}] \\
& -\begin{pmatrix} 2^{n-m} \\ 2 \end{pmatrix} \times [\begin{pmatrix} 2^m \\ 2 \end{pmatrix} - 2^{m-1}] \times 2^m\}2^{2^{n-1}-2^{n-m}+x-1}
\end{aligned}$$

□

Finally we consider the category for $1 \le c \le 2^{r-2} - 1$.

Lemma 2.3.5 Let $L(r,c) = 2^n - 2^r + c, 3 \le r \le n, 1 \le c \le 2^{r-2} - 1$, and $N_3(L(r,c))$ be the number of 2^n-periodic binary sequences with linear complexity 2^n and the 3-error linear complexity $L(r,c)$. Then

$$N_3(L) = \begin{cases} \begin{pmatrix} 2^n \\ 3 \end{pmatrix} + 2^n, & L = 0 \\ 2^{L-1}(\begin{pmatrix} 2^r \\ 3 \end{pmatrix} + 2^r), & L = L(r,c) \end{cases}$$

Proof. Suppose that s is a binary sequence with first period $s^{(n)} = \{s_0, s_1, s_2, \cdots, s_{2^n-1}\}$, and $L(s) = 2^n$. By the Games-Chan algorithm, $Left(s^{(t)}) \neq Right(s^{(t)}), 1 \le t \le n, L(s^{(0)}) = 1$, where $s^{(t)} = \varphi_{t+1} \cdots \varphi_n(s^{(n)})$.

Thus $s^{(0)} = \{1\}$, and $s_0 + s_1 + \cdots + s_{2^t-1} = 1, 1 \leq t \leq n$

First we consider the case of $W(s^{(n)}) = 1$. There is only one nonzero bit in $\{s_0, s_1, \cdots, s_{2^n-1}\}$, thus there are 2^n binary sequences of this kind.

Next, we consider the case of $W(s^{(n)}) = 3$. There are 3 nonzero bits in $\{s_0, s_1, \cdots, s_{2^n-1}\}$, thus there are $\begin{pmatrix} 2^n \\ 3 \end{pmatrix}$ binary sequences of this kind. So $N_3(0) = \begin{pmatrix} 2^n \\ 3 \end{pmatrix} + 2^n$.

Finally, we consider the case of $L(r, c) = 2^n - 2^r + c$, $3 \leq r \leq n, 1 \leq c \leq 2^{r-2} - 1$. Suppose that $s^{(n)}$ is a binary sequence with $L(s^{(n)}) = L(r, c)$. Note that $L(r, c) = 2^n - 2^r + c = 2^{n-1} + \cdots + 2^r + c$. By the Games-Chan algorithm (Games and Chan, 1983), $Left(s^{(r)}) = Right(s^{(r)})$, and $L(s^{(r)}) = c$.

It is known that the number of binary sequences $t^{(r)}$ with $W(t^{(r)}) = 1$ or 3 and $L(t^{(r)}) = 2^r$ is $\begin{pmatrix} 2^r \\ 3 \end{pmatrix} + 2^r$.

By Lemma 2.3.1, the 3-error linear complexity of $s^{(r)} + t^{(r)}$ is c.

By Lemma 2.1.6 in Section 2.1 and Lemma 2.3.2, the number of binary sequences $s^{(r)} + t^{(r)}$ is $2^{c-1} \times (\begin{pmatrix} 2^r \\ 3 \end{pmatrix} + 2^r)$

By Lemma 2.1.5 in Section 2.1, there are $2^{2^{n-1}+\cdots+2^r} = 2^{2^n-2^r}$ binary sequences $s^{(n)} + t^{(n)}$, such that $s^{(r)} + t^{(r)} = \varphi_{r+1} \cdots \varphi_n(s^{(n)} + t^{(n)})$, $t^{(r)} = \varphi_{r+1} \cdots \varphi_n(t^{(n)})$ and $W(t^{(n)}) = W(t^{(r)})$.

Thus the 3-error linear complexity of $s^{(n)} + t^{(n)}$ is

$$2^{n-1} + \cdots + 2^r + L_3(s^{(r)} + t^{(r)}) = 2^n - 2^r + c = L(r, c).$$

Therefore, $N_3(L(r, c)) = 2^{2^n-2^r} \times 2^{c-1} \times (\begin{pmatrix} 2^r \\ 3 \end{pmatrix} + 2^r) = 2^{L(r,c)-1}(\begin{pmatrix} 2^r \\ 3 \end{pmatrix} + 2^r)$ □

Based on the results above, we can have the proof of Theorem 2.3.1.

Proof. By Lemma 2.3.5, we now only need to consider the case of $4 \leq r \leq n, 2^{r-2} \leq c \leq 2^{r-1} - 1$.

By Lemma 2.1.5 in Section 2.1 and Lemma 2.3.3, $N_3(L(r,c)) = 2^{L(r,c)-1} f(r,m)$ for $4 \leq r \leq n, c = 2^{r-1} - 2^{r-m}, 1 < m \leq r$

By Lemma 2.1.5 in Section 2.1 and Lemma 2.3.4, $N_3(L(r,c)) = 2^{L(r,c)-1} g(r,m)$ for $4 \leq r \leq n, c = 2^{r-1} - 2^{r-m} + x, 1 < m < r-1, 0 < x < 2^{r-m-1}$ □

2.4 Complete counting functions for the 2-error or 3-error linear complexity

Based on previous investigations, we will give the complete counting functions for 2^n-period sequences with the 2-error or 3-error linear complexity. For completeness of presentation, the following theorem on the 1-error linear complexity from Meidl (2005) is given first.

Theorem 2.4.1 Let $L(r,c) = 2^n - 2^r + c, 2 \leq r \leq n, 1 \leq c \leq 2^{r-1} - 1$, and $N_1(L(r,c))$ be the number of 2^n-periodic binary sequences with linear complexity 2^n and the 1-error linear complexity $L(r,c)$. Then

$$N_1(L) = \begin{cases} 2^n, & L = 0 \\ 2^{L+r-1}, & L = L(r,c) \\ 0, & \text{otherwise} \end{cases}$$

From Theorem 2.4.1, we can have counting functions for the 2-error linear complexity of 2^n-periodic binary sequences with linear complexity 2^n. From Theorem 2.2.1, we have counting functions for the 2-error linear complexity of 2^n-periodic binary sequences with linear complexity less than 2^n. By combining these results of the two cases, it is easy to derive the complete counting functions for the number of 2^n-periodic binary sequences with the 2-error linear complexity.

Theorem 2.4.2 Let $L(r,c) = 2^n - 2^r + c$, $2 \le r \le n, 1 \le c \le 2^{r-1} - 1$, and $N_2(L(r,c))$ be the number of 2^n-periodic binary sequences with the 2-error linear complexity $L(r,c)$. Then

$$N_2(L) = \begin{cases} \binom{2^n}{2} + 2^n + 1, & L = 0 \\ 2^{L-1}(\binom{2^r}{2} + 2^r + 1), & \\ \qquad L = L(r,c), 1 \le c \le 2^{r-2} - 1, r > 2 & \\ 2^{L-1}(\binom{2^r}{2} + 2^r + 1 - 3 \times 2^{r+m-3}), & \\ \qquad L = L(r,c), c = 2^{r-1} - 2^{r-m}, 1 < m \le r, r \ge 2 & \\ 2^{L-1}(\binom{2^r}{2} + 2^r + 1 + 2^{r-m} - 2^{r+m-2}), & \\ \qquad L = L(r,c), c = 2^{r-1} - 2^{r-m} + x, 1 < m < r-1, 0 < x < 2^{r-m-1}, r > 3 & \\ 0, \qquad \text{otherwise} & \end{cases}$$

One can show that Theorem 2.4.2 is equivalent to the results in Table 1 and Table 2 by Kavuluru (2009).

Similarly, based on Theorem 2.2.1 and Theorem 2.3.1, the counting functions for the number of 2^n-periodic binary sequences with the 3-error linear complexity can be derived as follows.

Theorem 2.4.3 Let $L(r,c) = 2^n - 2^r + c$, $4 \le r \le n, 1 \le c \le 2^{r-1} - 1$, and $N_3(L(r,c))$ be the number of 2^n-periodic binary sequences with the 3-error linear complexity $L(r,c)$. Then

$$N_3(L) = \begin{cases} \binom{2^n}{3} + \binom{2^n}{2} + 2^n + 1, & L = 0 \\ 2^{L-1}(\binom{2^r}{3} + \binom{2^r}{2} + 2^r + 1), & \\ \qquad L = L(r,c), 1 \le c \le 2^{r-2} - 1, r > 3 & \\ 2^{L-1}(\binom{2^r}{2} + 1 - 3 \times 2^{r+m-3} + f(r,m)), & \\ \qquad L = L(r,c), c = 2^{r-1} - 2^{r-m}, 1 < m \le r, r > 3 & \\ 2^{L-1}(\binom{2^r}{2} + 1 + 2^{r-m} - 2^{r+m-2} + g(r,m)), & \\ \qquad L = L(r,c), c = 2^{r-1} - 2^{r-m} + x, 1 < m < r-1, 0 < x < 2^{r-m-1}, r > 3 & \\ 0, \qquad \text{otherwise} & \end{cases}$$

where $f(r,m)$ and $g(r,m)$ are defined in Theorem 2.3.1.

According to Table 1 and Table 2 by Kavuluru (2009), the numbers of 2^n-periodic binary sequences with the 3-error linear complexity for $n = 4$ are shown in the second column of Table 2.1.

Table 2.1: $N_3(L(r,c))$ by Kavuluru and Theorem 2.4.3.

$L(r,c)$	by Kavuluru	by Theorem 2.4.3
0	697	697
1	697	697
2	1394	1394
3	2788	2788
4	5128	2824
5	10704	8400
6	18720	4384
7	30272	2624
8	0	0
9	23808	23808
10	22016	8704
11	37888	5120
12	0	0
13	4096	4096
14	0	0
15	0	0

It is well known that the number of all 2^n-periodic binary sequences for $n = 4$ is $2^{16} = 65536$. However, the summation of numbers of the second column is much bigger than 65536. So the counting functions for the number of 2^n-periodic binary sequences with the 3-error linear complexity by Kavuluru (2009) are not fully correct.

Specifically, it is easy to check by computer that all underline numbers in Table 2.1 are incorrect.

In the case of $L = L(r, c), c = 2^{r-1} - 2^{r-m}, 1 < m \leq r, r \geq 2$, which corresponds to the case of $2^n - (2^{n-r_1} + 2^{n-r_2})$ by Kavuluru (2009), the counting function by Kavuluru (2009) is wrong.

$L = 4, 6, 7, 10$ or 11 in Table 2.1 belong to this case.

In the case of $L = L(r, c), c = 2^{r-1} - 2^{r-m} + x, 1 < m < r - 1, 0 < x < 2^{r-m-1}, r > 3$, which corresponds to the case of $2^n - (2^{n-r_1} + 2^{n-r_2}) < L < 2^n - (2^{n-r_1} + 2^{n-r_2-1})$ by Kavuluru (2009), the counting function by Kavuluru (2009) is wrong.

$L = 5$ in Table 2.1 is this case.

For $n = 4, L = 5$, we know that $r_1 = 1, r_2 = 2$, and

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

From Theorem 7 by Kavuluru (2008), we have $N_3(L) = 10704$, which is incorrect by computer check.

From Theorem 2.4.3, the numbers of 2^n-periodic binary sequences with the 3-error linear complexity for $n = 4$ are shown in the third column of Table 2.1. These results have been checked by computer.

The summation of numbers of the third column is $2^{16} = 65536$.

2.5 Counting functions for the 4-error linear complexity

By Theorem 2.3.1 in Section 2.3, the 3-error linear complexity of 2^n-periodic binary sequences with *linear complexity* 2^n has been investigated. For 2^n-periodic binary sequences with *linear complexity* 2^n, the change of 4 bits per period will result in a sequence with an odd number of nonzero bits per period, hence still with linear complexity 2^n. Therefore, the 4-error linear complexity is the same as the 3-error linear complexity for 2^n-periodic binary sequences in the case of *linear complexity* 2^n. In order to derive the counting functions for the 4-error linear complexity of 2^n-periodic binary sequences in general, we

only need to obtain the counting functions for the 4-error linear complexity of 2^n-periodic binary sequences with *linear complexity less than* 2^n. To this end, we divide the 4-error linear complexity into six non trivial categories and deal with them respectively.

First we consider the category of sequences with 4-error linear complexity $2^{n-2} - 2^{n-m}$.

Lemma 2.5.1 Let $N_4(2^{n-2} - 2^{n-m})$ be the number of 2^n-periodic binary sequences with *linear complexity less than* 2^n and the 4-error linear complexity $2^{n-2} - 2^{n-m}, n > 2, 2 < m \leq n$. Then

$$N_4(2^{n-2} - 2^{n-m}) = \left[1 + \binom{2^n}{2} + \binom{2^n}{4} - C1 - C2/2 \right] \times 2^{2^{n-2}-2^{n-m}-1}$$

where C1, C2 are defined in the following proof.

Proof. By Lemma 2.1.6 in Section 2.1, the number of 2^n-periodic binary sequences with linear complexity $2^{n-2} - 2^{n-m}$ is $2^{2^{n-2}-2^{n-m}-1}$. As the number of 2^n-periodic binary sequences in E is $1 + \binom{2^n}{2} + \binom{2^n}{4}$, the number of 2^n-periodic binary sequences $s + e \in S + E$ is at most $(1 + \binom{2^n}{2} + \binom{2^n}{4})2^{2^{n-2}-2^{n-m}-1}$.

We first characterize the set $LESS$. Assume that $u^{(n)}$ and $v^{(n)}$ are two distinct binary sequences with $W_H(u^{(n)}) = W_H(v^{(n)}) = 4$, and $L(u^{(n)} + v^{(n)}) = 2^{n-2} - 2^{n-m}$. Then the 4-error linear complexity of $u^{(n)} + s^{(n)}$ must be less than $2^{n-2} - 2^{n-m}$, where $L(s^{(n)}) = 2^{n-2} - 2^{n-m}$.

Suppose that $w^{(n)}$ is a binary sequence with linear complexity $2^{n-2}-2^{n-m}$ and $W_H(w^{(n)}) = 8$. Then $w^{(n)}$ can be divided into 4 equal parts and the number of such sequences is given by

$$(2^{n-2} - 2^{n-m}) + (2^{n-2} - 2^{n-m} \times 3) + \cdots + [2^{n-2} - 2^{n-m} \times (\frac{2^{n-2}}{2^{n-m}} - 1)] = 2^{n+m-6}.$$

Each $w^{(n)}$ has the intersection of 4 nonzero elements with $2(\frac{2^{n-2}}{2\times 2^{n-m}} - 1) = 2(2^{m-3} - 1)$ other different $w^{(n)}$. All these 4-nonzero-elements constitute the set

$$A_1 = \{(a_i, a_{i+2^{n-2}}, a_{i+2^{n-1}}, a_{i+2^{n-1}+2^{n-2}}) |\ 0 \leq i < 2^{n-2}\}$$

If the 4 nonzero elements of $u^{(n)}$ are part of 8 nonzero elements in one $w^{(n)}$, where

$W_H(w^{(n)}) = 8$, then the number of these $u^{(n)}$ is given by

$$C1 = 2^{n+m-6} \begin{pmatrix} 8 \\ 4 \end{pmatrix} - 2^{n-2}(2^{m-3} - 1).$$

Note that the second item in $C1$ implies that the 4 nonzero elements of $u^{(n)}$ can be in A_1.

Second, we characterize the set $EQUAL$. Suppose that $L_4(s^{(n)} + u^{(n)}) = L_4(t^{(n)} + v^{(n)}) = 2^{n-2} - 2^{n-m}$ with $s^{(n)} \neq t^{(n)}$, $u^{(n)} \neq v^{(n)}$, but $s^{(n)} + u^{(n)} = t^{(n)} + v^{(n)}$. Then $L(u^{(n)} + v^{(n)}) = L(s^{(n)} + t^{(n)}) < 2^{n-2} - 2^{n-m}$, where $L(s^{(n)}) = L(t^{(n)}) = 2^{n-2} - 2^{n-m}$.

Suppose that $w^{(n)}$ is a binary sequence with linear complexity $2^{n-2} - 2^{n-k}$, $2 < k < m$, and $W_H(w^{(n)}) = 8$. We define A_2 as the set of these sequences. So the number of these sequences is given by $|A_2| = 2^{n+k-6}$.

If the 4 nonzero bits of $u^{(n)}$ are part of $w^{(n)} \in A_2$, but does not belong to A_1, then the number of these $u^{(n)}$ can be given by $2^{n+k-6}[\begin{pmatrix} 8 \\ 4 \end{pmatrix} - 2]$.

In summary, for $2 < k < m$, the total number of $u^{(n)}$ is given by

$$C2 = \sum_{k=3}^{m-1} 2^{n+k-6}(\begin{pmatrix} 8 \\ 4 \end{pmatrix} - 2) = (2^{n+m-6} - 2^{n-3})(\begin{pmatrix} 8 \\ 4 \end{pmatrix} - 2).$$

For each of these $u^{(n)}$, there exists exactly one binary sequence $v^{(n)}$ with $W_H(v^{(n)}) = 4$, such that $L(u^{(n)} + v^{(n)}) = 2^{n-2} - 2^{n-k}$, $2 < k < m$. Let $t^{(n)} = s^{(n)} + u^{(n)} + v^{(n)}$. Then $L(t^{(n)}) = L(s^{(n)}) = 2^{n-2} - 2^{n-m}$ and $t^{(n)} + v^{(n)} = s^{(n)} + u^{(n)}$.

As the number of sequences in $LESS$ is $C1$ and the number of sequences in $EQUAL$ is $C2$, thus

$$N_4(2^{n-2} - 2^{n-m}) = [1 + \begin{pmatrix} 2^n \\ 2 \end{pmatrix} + \begin{pmatrix} 2^n \\ 4 \end{pmatrix} - C1 - C2/2] \times 2^{2^{n-2} - 2^{n-m} - 1}$$

□

Now we define $N_4(2^{n-2} - 2^{n-m}) = f(n, m) \times 2^{2^{n-2} - 2^{n-m} - 1}$ with notation $f(n, m)$. Next we consider the category of sequences with 4-error linear complexity $2^{n-2} - 2^{n-m} + x$.

Lemma 2.5.2 Let $N_4(2^{n-2}-2^{n-m}+x)$ be the number of 2^n-periodic binary sequences with *linear complexity less than* 2^n and the 4-error linear complexity $2^{n-2}-2^{n-m}+x, n > 4, 2 < m < n-1, 0 < x < 2^{n-m-1}$. Then

$$\begin{aligned} N_4(2^{n-2}-2^{n-m}+x) &= [1+\binom{2^n}{2}+\binom{2^n}{4}-2^{n-3}+2^{n-m} \\ &\quad -\frac{1}{2}(C1+C2)] \times 2^{2^{n-2}-2^{n-m}+x-1} \end{aligned}$$

where C1, C2 are defined in Lemma 2.5.1.

Proof. Suppose that $s^{(n)}$ is a binary sequence with linear complexity

$$2^{n-2}-2^{n-m}+x = 2^{n-1}-(2^{n-2}+2^{n-m})+x,$$

and $u^{(n)}$ is a binary sequence with $W_H(u^{(n)}) = 0, 2$ or 4. By Lemma 2.9, the 4-error linear complexity of $s^{(n)}+u^{(n)}$ is still $2^{n-2}-2^{n-m}+x$. So, we only need to characterize the set $EQUAL$.

Based on the proof of Lemma 3.1, there are $C1$ distinct binary sequences $u^{(n)}$ with $W_H(u^{(n)}) = 4$, such that $L(u^{(n)}+v^{(n)}) = 2^{n-2}-2^{n-m} < 2^{n-2}-2^{n-m}+x$, where $v^{(n)}$ is a binary sequence with $W_H(v^{(n)}) = 4$.

Among $C1$ binary sequences $u^{(n)}$ in set $LESS$, there are 2^{n-2} binary sequences with 4 nonzero elements in $A1$. For each of these sequences $u^{(n)}$, there exist $\sum_{k=3}^{m} \frac{2^{n-2}}{2^{n-k+1}} = \sum_{k=3}^{m} 2^{k-3} = 2^{m-2}-1$ distinct binary sequences $v^{(n)}$ with $W_H(v^{(n)}) = 4$, such that $L(u^{(n)}+v^{(n)}) = 2^{n-2}-2^{n-k}$, $2 < k \le m$. For each of other sequences $u^{(n)}$ in set $LESS$, there exists only one binary sequence $v^{(n)}$ with $W_H(v^{(n)}) = 4$, such that $L(u^{(n)}+v^{(n)}) = 2^{n-2}-2^{n-m}$.

For each of these $C2$ binary sequences $u^{(n)}$, there exists exactly one binary sequence $v^{(n)}$ with $W_H(v^{(n)}) = 4$, such that $L(u^{(n)}+v^{(n)}) = 2^{n-2}-2^{n-k}$, $2 < k < m$.

Therefore, the number of sequences in $EQUAL$ is $2^{n-2}+(C1-2^{n-2})+C2$, thus

$$\begin{aligned} N_4(2^{n-2}-2^{n-m}+x) &= [1+\binom{2^n}{2}+\binom{2^n}{4}-\frac{2^{m-2}-1}{2^{m-2}}2^{n-2} \\ &\quad -\frac{1}{2}(C1+C2-2^{n-2})] \times 2^{2^{n-2}-2^{n-m}+x-1} \end{aligned}$$

□

Similarly we can define $N_4(2^{n-2}-2^{n-m}+x) = g(n,m) \times 2^{2^{n-2}-2^{n-m}+x-1}$ with notation $g(n,m)$. Now we consider the category of sequences with 4-error linear complexity $2^{n-1}-2^{n-m}$.

Lemma 2.5.3 Let $N_4(2^{n-1}-2^{n-m})$ be the number of 2^n-periodic binary sequences with *linear complexity less than* 2^n and the 4-error linear complexity $2^{n-1}-2^{n-m}, 2 \le m \le n$. Then

$$N_4(2^{n-1}-2^{n-m}) = [\begin{pmatrix} 2^n \\ 4 \end{pmatrix} - E1 + E2/4 - E3 + E4/2 - E5 + E6/4 - E7 + E8/8] \times 2^{2^{n-1}-2^{n-m}-1}$$

where $E1, E2, \cdots, E8$ are defined in the following proof.

Proof. Suppose that $s^{(n)} = 2^{n-1}-2^{n-m}$, and $u^{(n)}$ is a binary sequence with $W_H(u^{(n)}) = 0$ or 2. One can verify that there exists a binary sequence $v^{(n)}$ with $W_H(v^{(n)}) = 4$, such that $L(u^{(n)}+v^{(n)}) = 2^{n-1}-2^{n-m}$. Then the 4-error linear complexity of $u^{(n)}+s^{(n)}$ is less than $2^{n-1}-2^{n-m}$.

Suppose that $u^{(n)}$ is a binary sequence with $W_H(u^{(n)}) = 4$. Let us divide one period of $u^{(n)}$ into 2^{n-m} subsequences with the following form

$$\{u_a, u_{a+2^{n-m}}, u_{a+2^{n-m+1}}, \cdots, u_{a+(2^m-1)\times 2^{n-m}}\}$$

where $0 \le a < 2^{n-m}$. Next we consider four cases depending on the nonzero element distribution in the subsequences of $u^{(n)}$.

Case 1): If only two nonzero elements of $u^{(n)}$ are in one subsequence and the other two nonzero elements are in another one, then the number of these $u^{(n)}$ is given by

$$E1 = \begin{pmatrix} 2^{n-m} \\ 2 \end{pmatrix} \times \begin{pmatrix} 2^m \\ 2 \end{pmatrix} \times \begin{pmatrix} 2^m \\ 2 \end{pmatrix}.$$

Among these $u^{(n)}$, if the distance of two nonzero bits in each subsequence is not $2^{n-m}(1+2a)$, $a \ge 0$, in other words, the two nonzero bits in each subsequence are both at odd locations or even locations, then the number of these $u^{(n)}$ is given by

$$\begin{pmatrix} 2^{n-m} \\ 2 \end{pmatrix} \times \begin{pmatrix} 2 \\ 1 \end{pmatrix} \times \begin{pmatrix} 2^{m-1} \\ 2 \end{pmatrix} \times \begin{pmatrix} 2 \\ 1 \end{pmatrix} \times \begin{pmatrix} 2^{m-1} \\ 2 \end{pmatrix}.$$

Also the number of sequences with exactly two nonzero elements and their distance equal to 2^{n-1}, is given by

$$\begin{pmatrix} 2^{n-m} \\ 2 \end{pmatrix} \times \begin{pmatrix} 2 \\ 1 \end{pmatrix} \times 2^{m-1} \times \begin{pmatrix} 2 \\ 1 \end{pmatrix} (\begin{pmatrix} 2^{m-1} \\ 2 \end{pmatrix} - 2^{m-2}).$$

and the number of sequences with at least two nonzero elements and their distance equal to 2^{n-1}, is given by

$$\left(\begin{array}{c} 2^{n-m} \\ 2 \end{array} \right) \times [2^{m-1} \times 2^{m-1} + 2^{m+1}(\left(\begin{array}{c} 2^{m-1} \\ 2 \end{array} \right) - 2^{m-2})]$$

So, if only two nonzero elements are in each subsequence, and their distance is neither $2^{n-m}(1+2a)$ nor 2^{n-1}, then the number of these $u^{(n)}$ is given by

$$\begin{aligned} E2 = 4 \times & \left(\begin{array}{c} 2^{n-m} \\ 2 \end{array} \right) \times \left(\begin{array}{c} 2^{m-1} \\ 2 \end{array} \right) \times \left(\begin{array}{c} 2^{m-1} \\ 2 \end{array} \right) \\ & - \left(\begin{array}{c} 2^{n-m} \\ 2 \end{array} \right) \times [2^{2m-2} + 2^{m+1}(\left(\begin{array}{c} 2^{m-1} \\ 2 \end{array} \right) - 2^{m-2})]. \end{aligned}$$

For each $u^{(n)}$, there exist 3 distinct sequences $v_i^{(n)}, 1 \le i \le 3$, with $W_H(v_i^{(n)}) = 4$, such that $L(u^{(n)} + v_i^{(n)}) = 2^{n-1} - 2^{n-r}$ or $2^{n-1} - (2^{n-r} + 2^{n-k}), 1 < r < m, m+1 \le k \le n$.

Case 2): If only two nonzero elements of $u^{(n)}$ are in one subsequence and the other two nonzero elements are in other two distinct subsequences, then the number of these $u^{(n)}$ is given by

$$E3 = \left(\begin{array}{c} 2^{n-m} \\ 3 \end{array} \right) \times \left(\begin{array}{c} 3 \\ 1 \end{array} \right) \times \left(\begin{array}{c} 2^{m} \\ 2 \end{array} \right) \times 2^m \times 2^m.$$

Among these $u^{(n)}$, the distance of the two nonzero bits which are in one subsequence is not $2^{n-m}(1+2a)$, then the number of these $u^{(n)}$ is given by $\left(\begin{array}{c} 2^{n-m} \\ 3 \end{array} \right) \times \left(\begin{array}{c} 3 \\ 1 \end{array} \right) \times (\left(\begin{array}{c} 2^{m-1} \\ 2 \end{array} \right) \times 2) \times 2^m \times 2^m$. Further note that the number of sequences, in which the distance of the two nonzero bits is 2^{n-1}, is given by

$$\left(\begin{array}{c} 2^{n-m} \\ 3 \end{array} \right) \times \left(\begin{array}{c} 3 \\ 1 \end{array} \right) \times 2^{m-1} \times 2^m \times 2^m.$$

So, if only two nonzero elements are in one subsequence, the other two nonzero elements are in other two distinct subsequences. The distances of the two nonzero elements in one subsequence is neither $2^{n-m}(1+2a)$ nor 2^{n-1}, then the number of these $u^{(n)}$ is given by

$$E4 = \left(\begin{array}{c} 2^{n-m} \\ 3 \end{array} \right) \left(\begin{array}{c} 3 \\ 1 \end{array} \right) \left(\begin{array}{c} 2^{m-1} \\ 2 \end{array} \right) \times 2^{2m+1} - \left(\begin{array}{c} 2^{n-m} \\ 3 \end{array} \right) \left(\begin{array}{c} 3 \\ 1 \end{array} \right) \times 2^{3m-1}.$$

Also we note that for each $u^{(n)}$ there exists one unique sequence $v^{(n)}$, with $W_H(v^{(n)}) = 4$, such that $L(u^{(n)} + v^{(n)}) = 2^{n-1} - 2^{n-r}$, $1 < r < m$.

Case 3): If there are only 3 nonzero elements in one subsequence, then the number of these $u^{(n)}$ is given by

$$E5 = \begin{pmatrix} 2^{n-m} \\ 2 \end{pmatrix} \begin{pmatrix} 2 \\ 1 \end{pmatrix} \begin{pmatrix} 2^m \\ 3 \end{pmatrix} \times 2^m.$$

Suppose that there are only three nonzero elements of $u^{(n)}$ in one subsequence, and there are no two nonzero bits with distance equal to $2^{n-m}(1 + 2a)$. Then the number of these $u^{(n)}$ is given by

$$\begin{pmatrix} 2^{n-m} \\ 2 \end{pmatrix} \begin{pmatrix} 2 \\ 1 \end{pmatrix} [\begin{pmatrix} 2^{m-1} \\ 3 \end{pmatrix} \times 2] \times 2^m$$

Among these $u^{(n)}$, there are

$$\begin{pmatrix} 2^{n-m} \\ 2 \end{pmatrix} \begin{pmatrix} 2 \\ 1 \end{pmatrix} [2^{m-1} \times (2^{m-1} - 2)] \times 2^m$$

sequences, in which there exist two nonzero elements with distance 2^{n-1}. So, if there are only 3 nonzero elements of $u^{(n)}$ in one subsequence, and there are no two nonzero elements with distance $2^{n-m}(1 + 2a)$ or 2^{n-1}, then the number of these $u^{(n)}$ can be given by

$$E6 = 2^{m+2} \times \begin{pmatrix} 2^{n-m} \\ 2 \end{pmatrix} \times \begin{pmatrix} 2^{m-1} \\ 3 \end{pmatrix} - \begin{pmatrix} 2^{n-m} \\ 2 \end{pmatrix} \times (2^{m-1} - 2) \times 2^{2m}.$$

Similarly for each $u^{(n)}$, there exist 3 distinct binary sequences $v_i^{(n)}, 1 \leq i \leq 3$, with $W_H(v_i^{(n)}) = 4$, such that $L(u^{(n)} + v_i^{(n)}) = 2^{n-1} - 2^{n-r}$, $1 < r < m$.

Case 4): If all 4 nonzero elements of $u^{(n)}$ are in one subsequence, then the number of these $u^{(n)}$ is given by

$$E7 = 2^{n-m} \times \begin{pmatrix} 2^m \\ 4 \end{pmatrix}.$$

Suppose that all 4 nonzero elements of $u^{(n)}$ are in one subsequence, and there are no two nonzero elements with distance $2^{n-m}(1 + 2a)$. Then the number of these $u^{(n)}$ is given by $2^{n-m} \times 2 \times \begin{pmatrix} 2^{m-1} \\ 4 \end{pmatrix}$.

Among these $u^{(n)}$, there are

$$2^{n-m} \times 2 \times 2^{m-2}[\begin{pmatrix} 2^{m-1}-2 \\ 2 \end{pmatrix} - 2^{m-2} + 1]$$

sequences, in which there exist exactly two nonzero elements with distance 2^{n-1}. Note that there are $2^{n-m+1} \times \begin{pmatrix} 2^{m-2} \\ 2 \end{pmatrix}$ sequences, in which there exist exactly 2 pairs of elements with distance 2^{n-1}. So we can obtain that there are

$$2^{n-1}\begin{pmatrix} 2^{m-1}-2 \\ 2 \end{pmatrix} - 2^{n-m+1} \times \begin{pmatrix} 2^{m-2} \\ 2 \end{pmatrix}$$

sequences, in which there exist at least two nonzero elements with distance 2^{n-1}.

So, if all four nonzero elements of $u^{(n)}$ are in one subsequence, and there are no two nonzero elements with distance $2^{n-m}(1+2a)$ or 2^{n-1}, then the number of these $u^{(n)}$ is given by

$$E8 = 2^{n-m+1} \times \begin{pmatrix} 2^{m-1} \\ 4 \end{pmatrix} - [2^{n-1} \times \begin{pmatrix} 2^{m-1}-2 \\ 2 \end{pmatrix} - 2^{n-m+1} \times \begin{pmatrix} 2^{m-2} \\ 2 \end{pmatrix}].$$

Further, one can show that there exist $\begin{pmatrix} 4 \\ 2 \end{pmatrix} + 1 = 7$ distinct binary sequences $v_i^{(n)}, 1 \leq i \leq 7$, with $W_H(v_i^{(n)}) = 4$, such that $L(u^{(n)} + v_i^{(n)}) = 2^{n-1} - 2^{n-r}$, $1 < r < m$ or $2^{n-1} - (2^{n-r} + 2^{n-k})$, $1 < r < k < m$.

Finally, as the number of sequences in $LESS$ is $(E1 - E2) + (E3 - E4) + (E5 - E6) + (E7 - E8)$ and the number of sequences in $EQUAL$ is $E2 + E4 + E6 + E8$, thus

$$\begin{aligned} & N_4(2^{n-1} - 2^{n-m}) \\ = \; & [\begin{pmatrix} 2^n \\ 4 \end{pmatrix} - (E1 - E2) - \frac{3}{4}E2 - (E3 - E4) - \frac{1}{2}E4 - (E5 - E6) \\ & -\frac{3}{4}E6 - (E7 - E8) - \frac{7}{8}E8] \times 2^{2^{n-1}-2^{n-m}-1} \\ = \; & [\begin{pmatrix} 2^n \\ 4 \end{pmatrix} - E1 + E2/4 - E3 + E4/2 - E5 + E6/4 - E7 + E8/8] \times 2^{2^{n-1}-2^{n-m}-1}. \end{aligned}$$

□

Now we rewrite $N_4(2^{n-1} - 2^{n-m}) = h(n,m) \times 2^{2^{n-1}-2^{n-m}-1}$ with notation $h(n,m)$. Next we present an important lemma, which will be used in proving our main result.

Lemma 2.5.4 Suppose that $s^{(n)}$ is a 2^n-periodic binary sequence with linear complexity $2^{n-1} - (2^{n-m} + 2^{n-j})$, $n > 3, 2 < m < j \leq n$, and $W_H(s^{(n)}) = 8$. Then the number of these $s^{(n)}$ is $2^{n+2m+j-10}$.

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

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

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

Based on the Games-Chan algorithm (Games and Chan, 1983), the number of these $s^{(n-m)}$ is given by $(2^2)^{n-m-(n-j)-1} \times 2^{n-j} = 2^{2(n-m)-(n-j)-2}$.

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

For $n-1 > n-m$, based on the Games-Chan algorithm, if 2^{n-1}-periodic binary sequences $s^{(n-1)}$ are with linear complexity $2^{n-1} - (2^{n-m} + 2^{n-j})$ and $W_H(s^{(n-1)}) = 4$, then the number of these $s^{(n-1)}$ is given by

$$(2^4)^{n-1-(n-m)-1} \times 2^{2(n-m)-(n-j)-2} = 2^{4(n-1)-2(n-m)-(n-j)-2-4} = 2^{n+2m+j-10}.$$

This completes the proof. □

Now it is time to investigate the category of sequences with 4-error linear complexity $2^{n-1} - (2^{n-m} + 2^{n-j})$. In order to simplify the complexity of the following proof for Lemma 2.5.5, we first analyze the possible decompositions and then give an outline for its proof as below.

It remains for us to investigate two cases. Case A is to exclude all sequences $s+u$ satisfying $s+u \in S+E$, but $L_4(s+u) < 2^{n-1} - (2^{n-m} + 2^{n-j})$. Based on Lemma 2.1.2 in Section 2.1, this is equivalent to checking if there exists a sequence v such that $L(u+v) = 2^{n-1} - (2^{n-m} + 2^{n-j})$, where $W_H(v) = 4$. Case B is to check the repetition of some sequences in $S+E$ satisfying that $s+u, t+v \in S+E$ and $L_4(s+u) = L_4(t+v) = 2^{n-1} - (2^{n-m} + 2^{n-j})$ with $s \neq t$, $u \neq v$, but $s+u = t+v$. Similarly, this is equivalent to checking if there exists a sequence v such that $L(u+v) = L(s+t) < 2^{n-1} - (2^{n-m} + 2^{n-j})$ and if so, check the number of such sequences. This is the first layer decomposition in Figure 2.1.

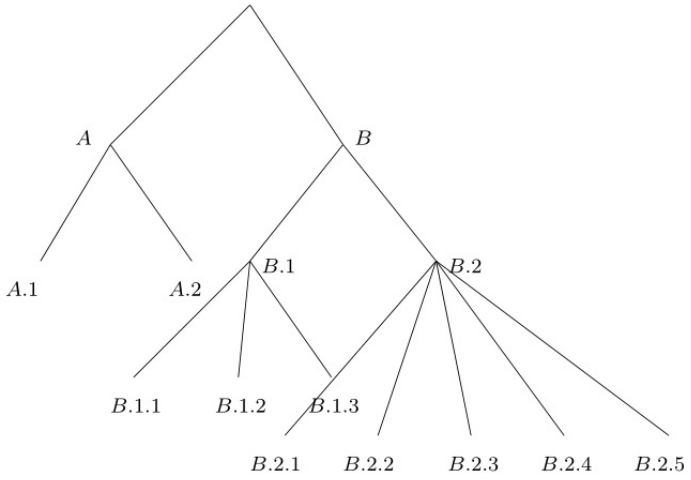

Figure 2.1: The decomposition of sequences with $L_4(s+u) = 2^{n-1} - (2^{n-m} + 2^{n-j})$

In Case A, we need to investigate the number of sequences $w^{(n)}$ satisfying $w^{(n)} = u^{(n)} + v^{(n)}$ with $L(w^{(n)}) = 2^{n-1} - (2^{n-m} + 2^{n-j})$ and $W_H(w^{(n)}) = 8, W_H(u^{(n)}) = 4$. Once we obtain the number of $w^{(n)}$, we need to derive the number of $u^{(n)}$. In order to exclude possible repetitions of $u^{(n)}$ with different $w^{(N)}$, we have two subcases to consider. Case A.1: $LH(u^{(n)}) = RH(u^{(n)})$. Case A.2: There are only two nonzero elements with distance 2^{n-1} among 4 nonzero elements of $u^{(n)}$. This is the decomposition under node A in Figure 2.1.

In Case B, there are also two subcases. Case B.1: we need to first find the number of sequences $w^{(n)}$ satisfying $w^{(n)} = u^{(n)} + v^{(n)}$ with $L(w^{(n)}) = 2^{n-1} - (2^{n-m} + 2^{n-k}) < 2^{n-1} - (2^{n-m} + 2^{n-j}), m < k < j$ and $W_H(w^{(n)}) = 8, W_H(u^{(n)}) = 4$. Case B.2: Consider sequence $u^{(n)}$ for which there is no binary sequence $v^{(n)}$, such that $L(u^{(n)} + v^{(n)}) = 2^{n-1} - (2^{n-m} + 2^{n-k}), m < k < j$. This is the decomposition under node B in Figure 2.1.

Similarly, we can decompose the Case B.1 into three subcases. Case B.1.1: $LH(u^{(n)}) = RH(u^{(n)})$. Case B.1.2: There are only 2 nonzero elements with distance 2^{n-1} among 4 nonzero elements of $u^{(n)}$. Case B.1.3: There are no two nonzero elements with distance 2^{n-1} among 4 nonzero elements of $u^{(n)}$.

In Case B.2, there are five subcases: Case B.2.1, Case B.2.2, Case B.2.3, Case B.2.4 and Case B.2.5.

The next step is to find all the number of sequences $u^{(n)}$ in all the nodes and there are total 10 leaves (cases). These cases are investigated one by one in Lemma 2.5.5.

Remark: In comparison with Lemma 2.3.3 in Section 2.3, for the 3-error linear complexity being equal to $2^{n-1} - 2^{n-m}$, there are only 4 leaves (cases) in the decomposition. The counting technique based on sieving is much more complicated in this section.

Next we will deal with all the cases in Figure 2.1 in Lemma 2.5.5.

Lemma 2.5.5 Let $N_4(2^{n-1}-(2^{n-m}+2^{n-j}))$ be the number of 2^n-periodic binary sequences with *linear complexity less than* 2^n and the 4-error linear complexity $2^{n-1} - (2^{n-m} + 2^{n-j}), n > 3, 2 < m < j \leq n$. Then

$$\begin{aligned}
& N_4(2^{n-1} - (2^{n-m} + 2^{n-j})) \\
= \; & [1 + \begin{pmatrix} 2^n \\ 2 \end{pmatrix} + \begin{pmatrix} 2^n \\ 4 \end{pmatrix} - F4 - \sum_{k=m+1}^{j-1} (\frac{2^{2m-3}-1}{2^{2m-3}} F6 + \frac{2^{m-1}-1}{2^{m-1}} F7 + F8/2) \\
& - \frac{2^{m-2}-1}{2^{m-2}} F10 - F11/2 - F13 - \frac{3}{4} F14 - \frac{2^{m-1}-1}{2^{m-1}} F17 - \frac{3}{4} F18 - \frac{2^{2m-4}-1}{2^{2m-4}} F19 \\
& - F22/2 - \frac{2^{m-2}-1}{2^{m-2}} F23 - F25 - F26 - \frac{7}{8} F27] \times 2^{2^{n-1}-(2^{n-m}+2^{n-j})-1}
\end{aligned}$$

where $F1, F2, \cdots, F27$ are defined in the following proof.

Proof. Suppose that $L(s^{(n)}) = 2^{n-1} - (2^{n-m} + 2^{n-j})$, $u^{(n)}$ is a binary sequence with $W_H(u^{(n)}) = 0$, 2 or 4. Then the number of these $u^{(n)}$ is given by $1 + \begin{pmatrix} 2^n \\ 2 \end{pmatrix} + \begin{pmatrix} 2^n \\ 4 \end{pmatrix}$.

Next we will investigate the $u^{(n)}$ by Case A) and Case B) separately.

Case A): Suppose that $w^{(n)}$ is a binary sequence with linear complexity $2^{n-1} - (2^{n-m} + 2^{n-j})$, and $W_H(w^{(n)}) = 8$. By Lemma 2.5.4, the number of these $w^{(n)}$ can be given by $2^{n+2m+j-10}$. Further by Lemma 2.1.9 in Section 2.1, there exist sequences $u^{(n)}$ and $v^{(n)}$ with $W_H(u^{(n)}) = W_H(v^{(n)}) = 4$, such that $L(u^{(n)} + v^{(n)}) = 2^{n-1} - (2^{n-m} + 2^{n-j})$, thus the 4-error linear complexity of $u^{(n)} + s^{(n)}$ is less than $2^{n-1} - (2^{n-m} + 2^{n-j})$.

Now suppose that $u^{(n)}$ is a binary sequence with $W_H(u^{(n)}) = 4$, and its 4 nonzero bits are part of the 8 nonzero elements in each $w^{(n)}$. There are totally $2^{n+2m+j-10} \times \begin{pmatrix} 8 \\ 4 \end{pmatrix}$ such sequences $u^{(n)}$, but some of which may be counted repeatedly. So we need to exclude these repetitions as discussed below.

Case A.1): $LH(u^{(n)}) = RH(u^{(n)})$. Among these $u^{(n)}$, if there exist two nonzero elements

in $LH(u^{(n)})$ with distance $2^{n-j}(1+2a)$, then the number of these $u^{(n)}$ is given by

$$F1 = 2^{n-j} \times \begin{pmatrix} 2^{j-1} \\ 2 \end{pmatrix} - 2^{n-j+1} \times \begin{pmatrix} 2^{j-2} \\ 2 \end{pmatrix} = 2^{n+j-4}.$$

One can observe that each of these $u^{(n)}$ is counted $\frac{2^{n-1}}{2^{n-m+1}} \times \frac{2^{n-1}}{2^{n-m+1}} = 2^{2(m-2)}$ times repeatedly in $2^{n+2m+j-10} \times \begin{pmatrix} 8 \\ 4 \end{pmatrix}$. This repetition is due to different choice of $w^{(n)}$ which can produce the same $u^{(n)}$.

Similarly, if the distance of two nonzero elements in $LH(u^{(n)})$ is $2^{n-m}(1+2a)$, then each of these $u^{(n)}$ is counted $2^{2(m-2)} \times \frac{2^{n-m}}{2^{n-j+1}} = 2^{m+j-5}$ times repeatedly in $2^{n+2m+j-10} \times \begin{pmatrix} 8 \\ 4 \end{pmatrix}$, and the number of these $u^{(n)}$ is given by

$$F2 = 2^{n-m} \begin{pmatrix} 2^{m-1} \\ 2 \end{pmatrix} - 2^{n-m+1} \begin{pmatrix} 2^{m-2} \\ 2 \end{pmatrix} = 2^{n+m-4}.$$

Case A.2): There are only two nonzero elements with distance 2^{n-1} among four nonzero elements of $u^{(n)}$. First we select three nonzero elements among four nonzero elements of $LH(w^{(n)})$, second, one selects two nonzero elements among these three nonzero elements and each of these two nonzero elements can be put in $LH(u^{(n)})$ or $RH(u^{(n)})$. So the number of these $u^{(n)}$ is given by

$$2^{n+2m+j-10} \begin{pmatrix} 4 \\ 3 \end{pmatrix} \begin{pmatrix} 3 \\ 2 \end{pmatrix} \times 2^2 = 3 \times 2^{n+2m+j-6}.$$

Similar to the first case, it is easy to verify that each of these $u^{(n)}$ is counted $\frac{2^{n-1}}{2^{n-m+1}} = 2^{m-2}$ times repeatedly. Suppose that $u^{(n)}$ is a binary sequence with $W_H(u^{(n)}) = 4$, and there are only two nonzero elements with distance 2^{n-1} among four nonzero elements of $u^{(n)}$. Then the number of these $u^{(n)}$ without repetition is given by

$$F3 = 3 \times 2^{n+2m+j-6}/2^{m-2} = 3 \times 2^{n+m+j-4}.$$

So, if the 4 nonzero elements of $u^{(n)}$ are part of the 8 nonzero elements in $w^{(n)}$, then there exists one unique binary sequence $v^{(n)}$ with $W_H(v^{(n)}) = 4$, such that $L(u^{(n)} + v^{(n)}) = 2^{n-1} - (2^{n-m} + 2^{n-j})$. So the 4-error linear complexity of $u^{(n)} + s^{(n)}$ is less than

$2^{n-1} - (2^{n-m} + 2^{n-j})$, and the number of these $u^{(n)}$ can be given by

$$\begin{aligned} F4 &= 2^{n+2m+j-10} \begin{pmatrix} 8 \\ 4 \end{pmatrix} - (2^{2(m-2)} - 1)F1 - (2^{m+j-5} - 1)F2 - (2^{m-2} - 1)F3 \\ &= 2^{n+2m+j-6} + 2^{n+m-4} + 2^{n+j-4} + 3 \times 2^{n+m+j-4}. \end{aligned}$$

Next we consider the case of $w^{(n)}$ with linear complexity less than $2^{n-1} - (2^{n-m} + 2^{n-j})$.

Case B): Consider $u^{(n)}$ for which there is no $v_1^{(n)}$, such that $L(u^{(n)}+v_1^{(n)}) = 2^{n-1}-(2^{n-m}+2^{n-j})$, but there exists $v^{(n)}$, such that $L(u^{(n)} + v^{(n)}) < 2^{n-1} - (2^{n-m} + 2^{n-j})$. In this case, let $t^{(n)} = s^{(n)}+u^{(n)}+v^{(n)}$, then $L(t^{(n)}) = 2^{n-1}-(2^{n-m}+2^{n-j})$, and $t^{(n)}+v^{(n)} = s^{(n)}+u^{(n)}$. Next we investigate two different cases based on the property of $u^{(n)}$.

Case B.1): We first investigate the case of a sequence $w^{(n)} = u^{(n)} + v^{(n)}$ with $L(w^{(n)}) = 2^{n-1} - (2^{n-m} + 2^{n-k}), m < k < j$ and $W_H(w^{(n)}) = 8$. By Lemma 3.4, the number of these $w^{(n)}$ is given by $2^{n+2m+k-10}$.

Suppose that $u^{(n)}$ is a binary sequence with $W_H(u^{(n)}) = 4$, and the 4 nonzero elements are part of the 8 nonzero elements of $w^{(n)}$. Then there are totally $2^{n+2m+k-10} \begin{pmatrix} 8 \\ 4 \end{pmatrix}$ such sequences $u^{(n)}$, some of which may be counted repeatedly. In order to exclude repetitions, we will investigate these $u^{(n)}$ by 3 subcases.

Case B.1.1): $LH(u^{(n)}) = RH(u^{(n)})$.

By Case A.1, if there exist two nonzero elements with distance $2^{n-m}(1 + 2a)$, then the number of these $u^{(n)}$ is given by

$$F5 = 2^{n+m-4}.$$

In this case, there exists a $v^{(n)}$, such that $L(u^{(n)} + v^{(n)}) = 2^{n-1} - (2^{n-m} + 2^{n-j})$. So there is no need to consider these $u^{(n)}$.

By Case A.1, if there exist two nonzero elements with distance $2^{n-k}(1 + 2a)$, then the number of these $u^{(n)}$ is given by

$$F6 = 2^{n+k-4}.$$

To be specific, there exist $2^{2(m-2)}$ distinct binary sequences $v^{(n)}$, such that $L(u^{(n)}+v^{(n)}) = 2^{n-1} - (2^{n-m} + 2^{n-k})$; there exist $(2^{m-2} - 1)^2$ distinct binary sequences $v^{(n)}$, such that

$L(u^{(n)}+v^{(n)}) = 2^{n-1} - (2^{n-m}+2^{n-k})$ or $2^{n-1} - 2^{n-i}$, $2 \le i < m$; there exist $2(2^{m-2}-1)$ distinct binary sequences $v^{(n)}$, such that $W_H(u^{(n)}+v^{(n)}) = 4$. So the number of distinct binary sequences $v_i^{(n)}, 1 \le i \le 2^{2m-3}-1$, with $W_H(v_i^{(n)}) = 4$, and $L(u^{(n)}+v_i^{(n)}) \le 2^{n-1} - (2^{n-m}+2^{n-k})$, is given by

$$2^{2(m-2)} + (2^{m-2}-1)^2 + 2(2^{m-2}-1) = 2^{2m-3} - 1.$$

Case B.1.2): There are only two nonzero elements with distance 2^{n-1}. By Case A.2), the number of these $u^{(n)}$ is given by

$$F7 = 3 \times 2^{n+m+k-4}.$$

To be specific, there exist 2^{m-2} distinct binary sequences $v^{(n)}$, such that $L(u^{(n)}+v^{(n)}) = 2^{n-1} - (2^{n-m}+2^{n-k})$; there exist $2^{m-2}-1$ distinct binary sequences $v^{(n)}$, such that $W_H(u^{(n)}+v^{(n)}) = 4$. So the number of distinct binary sequences $v_i^{(n)}, 1 \le i \le 2^{m-1}-1$, with $W_H(v_i^{(n)}) = 4$, and $L(u^{(n)}+v_i^{(n)}) \le 2^{n-1} - (2^{n-m}+2^{n-k})$, is given by

$$2^{m-2} + 2^{m-2} - 1 = 2^{m-1} - 1.$$

Case B.1.3): If there are no two nonzero elements with distance 2^{n-1}, then the number of these $u^{(n)}$ is given by

$$F8 = 2^{n+2m+k-10} \times 2^4 = 2^{n+2m+k-6}.$$

For each $u^{(n)}$, there exists one unique binary sequence $v^{(n)}$, with $W_H(v^{(n)}) = 4$, such that $L(u^{(n)}+v^{(n)}) = 2^{n-1} - (2^{n-m}+2^{n-k}) < 2^{n-1} - (2^{n-m}+2^{n-j}), m < k < j$.

Case B.2): Consider the sequence $u^{(n)}$ for which there is no binary sequence $v^{(n)}$, such that $L(u^{(n)}+v^{(n)}) = 2^{n-1} - (2^{n-m}+2^{n-k}), m < k < j$.

Let us divide one period of such $u^{(n)}$ into 2^{n-m+1} subsequences with the following form

$$\{u_a, u_{a+2^{n-m+1}}, u_{a+2^{n-m+2}}, \cdots, u_{a+(2^{m-1}-1)\times 2^{n-m+1}}\}$$

where $0 \le a < 2^{n-m+1}$.

Case B.2.1): Suppose that $u^{(n)}$ is a 2^n-periodic binary sequence with $W_H(u^{(n)}) = 2$, and all two nonzero elements are in one subsequence. Then the number of these $u^{(n)}$ is given by

$$F9 = 2^{n-m+1} \begin{pmatrix} 2^{m-1} \\ 2 \end{pmatrix}.$$

Among these $u^{(n)}$, there are $F10 = 2^{n-1}$ sequences, in which the distance of the 2 nonzero elements is 2^{n-1}. Also for each of these $u^{(n)}$, there exist

$$\frac{2^{n-1}}{2 \times 2^{n-2}} + \frac{2^{n-1}}{2 \times 2^{n-3}} + \cdots + \frac{2^{n-1}}{2 \times 2^{n-m+1}} = 2^{m-2} - 1$$

distinct binary sequences $v_i^{(n)}, 1 \le i \le 2^{m-2} - 1$, with $W_H(v_i^{(n)}) = 2$, such that $L(u^{(n)} + v_i^{(n)}) = 2^{n-1} - 2^{n-r}, 1 < r < m$.

So, if the two nonzero elements of $u^{(n)}$ are in one subsequence, and the distance of the 2 nonzero elements is not 2^{n-1}, then the number of these $u^{(n)}$ is given by $F11 = F9 - F10$. For each of these $u^{(n)}$, there exists one unique binary sequence $v^{(n)}$ with $W_H(v^{(n)}) = 2$, such that $L(u^{(n)} + v^{(n)}) = 2^{n-1} - 2^{n-r}, 1 < r < m$.

Case B.2.2): Suppose that $u^{(n)}$ is a 2^n-periodic binary sequence with $W_H(u^{(n)}) = 4$, and only three nonzero elements are in one subsequence. Then there exist at least one pair of nonzero elements with distance $2^{n-i}(1 + 2a), 1 < i < m, a \ge 0$. Thus $u^{(n)}$ is not in Case B.1). So the number of these $u^{(n)}$ is given by

$$F12 = \begin{pmatrix} 2^{n-m+1} \\ 2 \end{pmatrix} \times \begin{pmatrix} 2 \\ 1 \end{pmatrix} \times \begin{pmatrix} 2^{m-1} \\ 3 \end{pmatrix} \times 2^{m-1}.$$

Among these $u^{(n)}$, there are

$$F13 = \begin{pmatrix} 2^{n-m+1} \\ 2 \end{pmatrix} \times \begin{pmatrix} 2 \\ 1 \end{pmatrix} \times 2^{m-2} \times (2^{m-1} - 2) \times 2^{m-1}$$

sequences, in which the distance of the two nonzero elements is 2^{n-1}. It is easy to verify that there exists a binary sequence $v^{(n)}$ with $W_H(v^{(n)}) = 2$, such that $L(u^{(n)} + v^{(n)}) = 2^{n-1} - 2^{n-r}, 1 < r < m$.

Let $t^{(n)} = s^{(n)} + u^{(n)} + v^{(n)}$, then $L(t^{(n)}) = 2^{n-1} - (2^{n-m} + 2^{n-j})$, and $t^{(n)} + v^{(n)} = s^{(n)} + u^{(n)}$, thus we only need to count $t^{(n)} + v^{(n)}$ with $W_H(v^{(n)}) = 2$.

So, if only three nonzero elements of $u^{(n)}$ are in one subsequence, and there are no two nonzero elements with distance 2^{n-1}, then the number of these $u^{(n)}$ can be given by $F14 =$

$F12 - F13$. Among these $u^{(n)}$, there exist 3 distinct binary sequences $v_i^{(n)}, 1 \le i \le 3$, with $W_H(v_i^{(n)}) = 4$, such that $W_H(u^{(n)} + v_i^{(n)}) = 4$ and $L(u^{(n)} + v_i^{(n)}) < 2^{n-1} - (2^{n-m} + 2^{n-j})$.

Case B.2.3): Suppose that $u^{(n)}$ is a 2^n-periodic binary sequence with $W_H(u^{(n)}) = 4$, and 2 nonzero elements are in one subsequence, and the other two nonzero elements are in a different one. Then the number of these $u^{(n)}$ can be given by

$$F15 = \begin{pmatrix} 2^{n-m+1} \\ 2 \end{pmatrix} \times \begin{pmatrix} 2^{m-1} \\ 2 \end{pmatrix}^2.$$

Among these $u^{(n)}$, if there exist 2 pairs of nonzero elements with distance 2^{n-1}, then the distance of 2 nonzero elements from different subsequences is $2^{n-i}(1+2a), m \le i \le n, a \ge 0$. If the 4 nonzero elements are in $w^{(n)}$, and $L(w^{(n)}) = 2^{n-1} - (2^{n-m} + 2^{n-k}), m < k \le j$, then the number of those $u^{(n)}$ is $F2 + \sum_{k=m+1}^{j} 2^{n+k-4}$ as discussed in Case A.1) and Case B.1.1). So the number of the remaining sequences $u^{(n)}$ can be given by

$$F16 = F15 - F2 - \sum_{k=m+1}^{j} 2^{n+k-4}.$$

Among these $u^{(n)}$, if there exist only 2 nonzero elements with distance 2^{n-1}, then the distance of other 2 nonzero elements is $2^{n-i}(1+2a), 1 < i < m, a \ge 0$. Thus $u^{(n)}$ is not in Case B.1). So the number of these $u^{(n)}$ is given by

$$F17 = \begin{pmatrix} 2^{n-m+1} \\ 2 \end{pmatrix} \times \begin{pmatrix} 2 \\ 1 \end{pmatrix} \times 2^{m-2} \times [\begin{pmatrix} 2^{m-1} \\ 2 \end{pmatrix} - 2^{m-2}].$$

For each $u^{(n)}$, there exist $(\frac{2^{n-1}}{2^{m+1}} - 1) \times 2 + 1 = 2^{m-1} - 1$ distinct binary sequences $v_i^{(n)}, 1 \le i \le 2^{m-1} - 1$, with $W_H(v_i^{(n)}) = 4$, such that $L(u^{(n)} + v_i^{(n)}) < 2^{n-1} - (2^{n-m} + 2^{n-j})$.

If the distance of 2 nonzero elements in each subsequence is not 2^{n-1}, then the number of these $u^{(n)}$ is given by

$$F18 = \begin{pmatrix} 2^{n-m+1} \\ 2 \end{pmatrix} \times [\begin{pmatrix} 2^{m-1} \\ 2 \end{pmatrix} - 2^{m-2}]^2.$$

There exist 3 distinct binary sequences $v_i^{(n)}, 1 \le i \le 3$, with $W_H(v_i^{(n)}) = 4$, such that $L(u^{(n)} + v_i^{(n)}) < 2^{n-1} - (2^{n-m} + 2^{n-j})$.

So, there are $F19 = F16 - F17 - F18$ sequences, in which the distance of 2 nonzero elements in each subsequence is 2^{n-1}, and the distance of 2 nonzero elements from different subsequences is $2^{n-k}(1+2a), j < k \leq n$. There exist $(\frac{2^{n-1}}{2^{n-m+1}} - 1)^2 + (\frac{2^{n-1}}{2^{n-m+1}} - 1) \times 2 = 2^{2m-4} - 1$ distinct binary sequences $v_i^{(n)}, 1 \leq i \leq 2^{2m-4} - 1$, with $W_H(v_i^{(n)}) = 4$, such that $L(u^{(n)} + v_i^{(n)}) < 2^{n-1} - (2^{n-m} + 2^{n-j})$.

Case B.2.4): Suppose that $u^{(n)}$ is a binary sequence with $W_H(u^{(n)}) = 4$ and 2 nonzero elements of $u^{(n)}$ are in one subsequence and the other 2 nonzero elements are in the other 2 distinct subsequences. Then the number of these $u^{(n)}$ can be given by

$$F20 = \begin{pmatrix} 2^{n-m+1} \\ 3 \end{pmatrix} \times \begin{pmatrix} 3 \\ 1 \end{pmatrix} \times \begin{pmatrix} 2^{m-1} \\ 2 \end{pmatrix} \times (2^{m-1})^2.$$

If the distance of 2 nonzero elements of the same subsequence is 2^{n-1}, then we need to remove some sequences $u^{(n)}$ already discussed in Case A.2) and Case B.1.2). The number of those $u^{(n)}$ is $3 \times 2^{n+m+k-4}$, and there exists a binary sequence $v^{(n)}$ with $W_H(v^{(n)}) = 4$, such that $L(u^{(n)} + v^{(n)}) = 2^{n-1} - (2^{n-m} + 2^{n-k}), m < k \leq j$. So the number of the remaining sequences $u^{(n)}$ is given by

$$F21 = F20 - 3 \sum_{k=m+1}^{j} 2^{n+m+k-4}.$$

Among these $u^{(n)}$, if there are no 2 nonzero elements with distance 2^{n-1}, then the number of these $u^{(n)}$ is given by

$$F22 = \begin{pmatrix} 2^{n-m+1} \\ 3 \end{pmatrix} \begin{pmatrix} 3 \\ 1 \end{pmatrix} \times [\begin{pmatrix} 2^{m-1} \\ 2 \end{pmatrix} - 2^{m-2}] \times (2^{m-1})^2.$$

For each of these $u^{(n)}$, there exists one binary sequence $v^{(n)}$, with $W_H(v^{(n)}) = 4$, such that $L(u^{(n)} + v^{(n)}) = 2^{n-1} - 2^{n-r}, 1 < r < m$.

So, if there exist 2 nonzero elements of $u^{(n)}$ with distance 2^{n-1}, and there is no binary sequence $v^{(n)}$ with $W_H(v^{(n)}) = 4$, such that $L(u^{(n)} + v^{(n)}) = 2^{n-1} - (2^{n-m} + 2^{n-k}), m < k \leq j$, then the number of these $u^{(n)}$ is given by

$$F23 = F21 - F22.$$

For each of these $u^{(n)}$, there exist $\frac{2^{n-1}}{2^{n-m+1}} - 1 = 2^{m-2} - 1$ distinct binary sequences $v_i^{(n)}, 1 \leq i \leq 2^{m-2} - 1$, with $W_H(v_i^{(n)}) = 4$, such that $L(u^{(n)} + v_i^{(n)}) = 2^{n-1} - 2^{n-r}, 1 < r < m$.

Case B.2.5): Suppose that $u^{(n)}$ is a binary sequence with $W_H(u^{(n)}) = 4$ and all 4 nonzero elements of $u^{(n)}$ are in one subsequence. Then the number of these $u^{(n)}$ is given by

$$F24 = 2^{n-m+1} \times \begin{pmatrix} 2^{m-1} \\ 4 \end{pmatrix}.$$

Among these $u^{(n)}$, there are

$$F25 = 2^{n-m+1} \times \begin{pmatrix} 2^{m-2} \\ 2 \end{pmatrix}$$

sequences, in which there exist nonzero elements z_1,z_2, z_3 and z_4, such that the distance of z_1 and z_2, and the distance of z_3 and z_4 are all 2^{n-1}.

For each of these $u^{(n)}$, there exists a binary sequence $v^{(n)}$ with $W_H(v^{(n)}) = 0$, such that $L(u^{(n)} + v^{(n)}) = 2^{n-1} - 2^{n-r}, 1 < r < m$. Let $t^{(n)} = s^{(n)} + u^{(n)} + v^{(n)} = s^{(n)} + u^{(n)}$, thus we only need to count $t^{(n)} + v^{(n)}$ with $W_H(v^{(n)}) = 0$.

If there are only 2 nonzero elements with distance 2^{n-1}, then the number of these $u^{(n)}$ is given by

$$F26 = 2^{n-m+1} \times 2^{m-2} \times [\begin{pmatrix} 2^{m-1} - 2 \\ 2 \end{pmatrix} - (2^{m-2} - 1)].$$

For each of these $u^{(n)}$, there exist 2 binary sequences $v^{(n)}$ with $W_H(v^{(n)}) = 2$, such that $L(u^{(n)} + v^{(n)}) = 2^{n-1} - 2^{n-r}, 1 < r < m$. Let $t^{(n)} = s^{(n)} + u^{(n)} + v^{(n)}$, then $L(t^{(n)}) = 2^{n-1} - (2^{n-m} + 2^{n-j})$, and $t^{(n)} + v^{(n)} = s^{(n)} + u^{(n)}$, thus we only need to count $t^{(n)} + v^{(n)}$ with $W_H(v^{(n)}) = 2$.

So, if there are no 2 nonzero elements with distance 2^{n-1}, then the number of these $u^{(n)}$ can be given by

$$F27 = F24 - F25 - F26.$$

For each of these $u^{(n)}$, there exist $\begin{pmatrix} 4 \\ 2 \end{pmatrix} + 1 = 7$ distinct binary sequences $v_i^{(n)}, 1 \leq i \leq 7$, with $W_H(v_i^{(n)}) = 4$, such that $L(u^{(n)} + v_i^{(n)}) < 2^{n-1} - (2^{n-m} + 2^{n-j})$.

Finally, we have that the number of sequences in $LESS$ is $F4$ and the number of sequences in $EQUAL$ is given by

$$F10+F11+F13+F14+F17+F18+F19+F22+F23+F25+F26+F27+\sum_{k=m+1}^{j-1}(F6+F7+F8).$$

Notice that in the cases including $F13, F25, F26$, we only need to count $t^{(n)} + v^{(n)}$ with $W_H(v^{(n)}) \neq W_H(u^{(n)})$, which leads to the following

$$\begin{aligned}
& N_4(2^{n-1} - (2^{n-m} + 2^{n-j})) \\
= \; & [1 + \left(\begin{array}{c} 2^n \\ 2 \end{array} \right) + \left(\begin{array}{c} 2^n \\ 4 \end{array} \right) - F4 - \sum_{k=m+1}^{j-1} (\frac{2^{2m-3}-1}{2^{2m-3}} F6 + \frac{2^{m-1}-1}{2^{m-1}} F7 + F8/2) \\
& - \frac{2^{m-2}-1}{2^{m-2}} F10 - F11/2 - F13 - \frac{3}{4} F14 - \frac{2^{m-1}-1}{2^{m-1}} F17 - \frac{3}{4} F18 - \frac{2^{2m-4}-1}{2^{2m-4}} F19 \\
& - F22/2 - \frac{2^{m-2}-1}{2^{m-2}} F23 - F25 - F26 - \frac{7}{8} F27] \times 2^{2^{n-1} - (2^{n-m} + 2^{n-j}) - 1}
\end{aligned}$$

□

Let us denote $N_4(2^{n-1} - (2^{n-m} + 2^{n-j})) = p(n, m, j) \times 2^{2^{n-1} - (2^{n-m} + 2^{n-j}) - 1}$ with notation $p(n, m, j)$. Now we investigate the category of sequences with the 4-error linear complexity $2^{n-1} - (2^{n-m} + 2^{n-j}) + x$.

Lemma 2.5.6 Let $N_4(2^{n-1} - (2^{n-m} + 2^{n-j}) + x)$ be the number of 2^n-periodic binary sequences with *linear complexity less than* 2^n and the 4-error linear complexity $2^{n-1} - (2^{n-m} + 2^{n-j}) + x, n > 5, 2 < m < j < n - 1, 1 \leq x < 2^{n-j-1}$. Then

$$\begin{aligned}
& N_4(2^{n-1} - (2^{n-m} + 2^{n-j}) + x) \\
= \; & [1 + \left(\begin{array}{c} 2^n \\ 2 \end{array} \right) + \left(\begin{array}{c} 2^n \\ 4 \end{array} \right) - 2^{n-j}(2^{m+j-4} - 1) \\
& - \sum_{k=m+1}^{j} (\frac{2^{2m-3}-1}{2^{2m-3}} F6 + \frac{2^{m-1}-1}{2^{m-1}} F7 + F8/2) \\
& - \frac{2^{m-2}-1}{2^{m-2}} F10 - F11/2 - F13 - \frac{3}{4} F14 - \frac{2^{m-1}-1}{2^{m-1}} F17 - \frac{3}{4} F18 - \frac{2^{2m-4}-1}{2^{2m-4}} F19 \\
& - F22/2 - \frac{2^{m-2}-1}{2^{m-2}} F23 - F25 - F26 - \frac{7}{8} F27] \times 2^{2^{n-1} - (2^{n-m} + 2^{n-j}) + x - 1}
\end{aligned}$$

where $F6, F7, \cdots, F27$ are defined in the proof of Lemma 2.5.5.

Proof. Suppose that $s^{(n)}$ is a binary sequence with linear complexity $2^{n-1} - (2^{n-m} + 2^{n-j}) + x$, $u^{(n)}$ is a binary sequence with $W_H(u^{(n)}) = 0, 2$ or 4. By Lemma 2.1.9 in Section 2.1, the 4-error linear complexity of $s^{(n)} + u^{(n)}$ is still $2^{n-1} - (2^{n-m} + 2^{n-j}) + x$. So, we only need to characterize the set $EQUAL$.

Based on the proof of Lemma 2.5.5, we only need to characterize these $F4$ binary sequences $u^{(n)}$ in set $LESS$. Suppose that $w^{(n)}$ is a 2^n-periodic sequence with linear complexity $2^{n-1} - (2^{n-m} + 2^{n-j})$ and $W_H(w^{(n)}) = 8$. Then $LESS = \{u^{(n)} | W_H(u^{(n)}) = 4$ and the 4 nonzero elements are part of the 8 nonzero elements of $w^{(n)}\}$

We will investigate these binary sequences $u^{(n)}$ by the following three cases.

Case 1): $LH(u^{(n)}) = RH(u^{(n)})$. Based on the proof of Lemma 3.5, the number of these $u^{(n)}$ can be given by $2^{n+m-4} + 2^{n+j-4}$.

Case 1.1): Among these $u^{(n)}$, if there exist 2 nonzero elements in $LH(u^{(n)})$ whose distance is $2^{n-m}(1+2a), a \geq 0$, and the number of these $u^{(n)}$ can be given by

$$G1 = 2^{n+m-4}$$

Suppose that $W_H(v^{(n)}) = 4$ and $L(u^{(n)} + v^{(n)}) < 2^{n-1} - (2^{n-m} + 2^{n-j}) + x$. We will investigate the number of these $v^{(n)}$ by the following 2 cases.

Case 1.1.1): $L(u^{(n)} + v^{(n)}) = 2^{n-1} - (2^{n-m} + 2^{n-k})$, $m < k \leq j$. By Case A.1) of Lemma 3.5, the number of these $v^{(n)}$ is 2^{m+k-5}.

Case 1.1.2): Let us divide $LH(u^{(n)})$ into 2^{n-m} subsequences. From the subsequence which contains the 2 nonzero elements of $LH(u^{(n)})$, we first select one location as one nonzero element of $LH(v^{(n)})$. The number of locations of another nonzero element in $LH(v^{(n)})$ is $\frac{2^{n-1}}{2^{n-m+1}}$, such that the distance of 2 nonzero elements of $LH(v^{(n)})$ is $2^{n-m}(1+2a), a \geq 0$.

As we select every $v^{(n)}$ twice and one $v^{(n)}$ is the same as $u^{(n)}$, thus the number of these $v^{(n)}$ is $\frac{1}{2}(\frac{2^{n-1}}{2^{n-m}} \times \frac{2^{n-1}}{2^{n-m+1}}) - 1 = 2^{2(m-2)} - 1$, such that $L(u^{(n)} + v^{(n)}) < 2^{n-1} - (2^{n-m} + 2^{n-j})$. Therefore, there exist

$$\sum_{k=m+1}^{j} 2^{m+k-5} + 2^{2(m-2)} - 1 = 2^{m+j-4} - 1$$

distinct binary sequences $v_i^{(n)}, 1 \leq i \leq 2^{m+j-4} - 1$, with $W_H(v_i^{(n)}) = 4$, such that $L(u^{(n)} + v_i^{(n)}) < 2^{n-1} - (2^{n-m} + 2^{n-j}) + x$.

Case 1.2): Based on the proof of Lemma 2.5.5, if there exist 2 nonzero elements in $LH(u^{(n)})$ with distance $2^{n-j}(1+2a)$, then the number of these $u^{(n)}$ can be given by

$$G2 = 2^{n+j-4}$$

Suppose that $W_H(v^{(n)}) = 4$ and $L(u^{(n)} + v^{(n)}) < 2^{n-1} - (2^{n-m} + 2^{n-j}) + x$. We will investigate the number of these $v^{(n)}$ by the following 2 cases.

Case 1.2.1): $L(u^{(n)} + v^{(n)}) = 2^{n-1} - (2^{n-m} + 2^{n-j})$. By Case A.1) of Lemma 2.5.5, the the number of these $v^{(n)}$ is $2^{2(m-2)}$.

Case 1.2.2): From the locations which have distance $2^{n-m}(2a), a \geq 0$ with the first nonzero element of $LH(u^{(n)})$, we first select one location as one nonzero element of $LH(v^{(n)})$. Then from the locations which have distance $2^{n-m}(2b), b \geq 0$ with the second nonzero element of $LH(u^{(n)})$, we select one location as another nonzero element of $LH(v^{(n)})$. As one $v^{(n)}$ is the same as $u^{(n)}$, thus the number of these $v^{(n)}$ is

$$(\frac{2^{n-1}}{2^{n-m+1}})^2 - 1 = 2^{2(m-2)} - 1,$$

such that $L(u^{(n)} + v^{(n)}) < 2^{n-1} - (2^{n-m} + 2^{n-j})$.

Therefore, there exist $2^{2(m-2)} + 2^{2(m-2)} - 1 = 2^{2m-3} - 1$ distinct binary sequences $v_i^{(n)}, 1 \leq i \leq 2^{2m-3} - 1$, with $W_H(v_i^{(n)}) = 4$, such that $L(u^{(n)} + v_i^{(n)}) < 2^{n-1} - (2^{n-m} + 2^{n-j}) + x$.

Case 2): There are only 2 nonzero elements with distance 2^{n-1}. By the proof of Lemma 2.5.5, the number of these $u^{(n)}$ can be given by

$$G3 = 3 \times 2^{n+m+j-4}$$

For each $u^{(n)}$, there exist

$$\frac{2^{n-1}}{2^{n-m+1}} + (\frac{2^{n-1}}{2^{n-m+1}} - 1) = 2^{m-1} - 1$$

distinct binary sequences $v_i^{(n)}, 1 \leq i \leq 2^{m-1} - 1$, with $W_H(v_i^{(n)}) = 4$, such that $L(u^{(n)} + v_i^{(n)}) < 2^{n-1} - (2^{n-m} + 2^{n-j}) + x$. There are $\frac{2^{n-1}}{2^{n-m+1}} - 1$ distinct binary sequences $v^{(n)}$, such that $W_H(u^{(n)} + v^{(n)}) = 4$.

Case 3): If there are no 2 nonzero elements with distance 2^{n-1}, then the number of these $u^{(n)}$ can be given by

$$G4 = 2^{n+2m+j-10} \times 2^4 = 2^{n+2m+j-6}$$

For each $u^{(n)}$, there exists one unique binary sequence $v^{(n)}$, with $W_H(v^{(n)}) = 4$, such that $L(u^{(n)} + v^{(n)}) = 2^{n-1} - (2^{n-m} + 2^{n-j})$.

Based on Case B) in the proof of Lemma 3.5, it is easy to have the following

$$\begin{aligned}
& N_4(2^{n-1}-(2^{n-m}+2^{n-j})+x) \\
= \; & [1+\left(\begin{array}{c} 2^n \\ 2 \end{array}\right)+\left(\begin{array}{c} 2^n \\ 4 \end{array}\right)-\frac{2^{m+j-4}-1}{2^{m+j-4}}G1-\frac{2^{2m-3}-1}{2^{2m-3}}G2-\frac{2^{m-1}-1}{2^{m-1}}G3-G4/2 \\
& -\sum_{k=m+1}^{j-1}(\frac{2^{2m-3}-1}{2^{2m-3}}F6+\frac{2^{m-1}-1}{2^{m-1}}F7+F8/2) \\
& -\frac{2^{m-2}-1}{2^{m-2}}F10-F11/2-F13-\frac{3}{4}F14-\frac{2^{m-1}-1}{2^{m-1}}F17-\frac{3}{4}F18-\frac{2^{2m-4}-1}{2^{2m-4}}F19 \\
& -F22/2-\frac{2^{m-2}-1}{2^{m-2}}F23-F25-F26-\frac{7}{8}F27]\times 2^{2^{n-1}-(2^{n-m}+2^{n-j})+x-1}
\end{aligned}$$

□

Finally, let $N_4(2^{n-1}-(2^{n-m}+2^{n-j})+x) = q(n,m,j)\times 2^{2^{n-1}-(2^{n-m}+2^{n-j})+x-1}$ with notation $q(n,m,j)$ and we have the following result.

Lemma 2.5.7 Let $L(r,c) = 2^n - 2^r + c, 4 \le r \le n, 1 \le c \le 2^{r-3}-1$, and $N_4(L)$ be the number of 2^n-periodic binary sequences with *linear complexity less than* 2^n and the 4-error linear complexity L. Then

$$N_4(L) = \begin{cases} 1+\left(\begin{array}{c} 2^n \\ 2 \end{array}\right)+\left(\begin{array}{c} 2^n \\ 4 \end{array}\right), & L=0 \\ 2^{L-1}(1+\left(\begin{array}{c} 2^r \\ 2 \end{array}\right)+\left(\begin{array}{c} 2^r \\ 4 \end{array}\right)), & L=L(r,c) \end{cases}$$

Proof. Suppose that s is a binary sequence with first period $s^{(n)} = \{s_0, s_1, s_2, \cdots, s_{2^n-1}\}$, and $L(s^{(n)}) = 2^n - 2^r + c$. By the Games-Chan algorithm (Games and Chan, 1983), $LH(s^{(t)}) \neq RH(s^{(t)}), r+1 \le t \le n$, where $s^{(t)} = \varphi_{t+1}\cdots\varphi_n(s^{(n)})$.

First we consider the case of $W_H(s^{(n)}) = 0$. There is only one such binary sequence. For the case of $W_H(s^{(n)}) = 2$. There are 2 nonzero bits in $\{s_0, s_1, \cdots, s_{2^n-1}\}$, thus there are $\left(\begin{array}{c} 2^n \\ 2 \end{array}\right)$ binary sequences. Similarly for the case of $W_H(s^{(n)}) = 4$. There are 4 nonzero bits in $\{s_0, s_1, \cdots, s_{2^n-1}\}$, thus there are $\left(\begin{array}{c} 2^n \\ 4 \end{array}\right)$ binary sequences. So $N_4(0) = 1+\left(\begin{array}{c} 2^n \\ 2 \end{array}\right)+\left(\begin{array}{c} 2^n \\ 4 \end{array}\right)$.

Consider the case of $L(r,c) = 2^n - 2^r + c$, $4 \le r \le n, 1 \le c \le 2^{r-3} - 1$. Suppose that $s^{(n)}$ is a binary sequence with $L(s^{(n)}) = L(r,c)$. Note that $L(r,c) = 2^n - 2^r + c = 2^{n-1} + \cdots + 2^r + c$. By the Games-Chan algorithm, $LH(s^{(r)}) = RH(s^{(r)})$, and $L(s^{(r)}) = c$.

It is known that the number of binary sequences $t^{(r)}$ with $W_H(t^{(r)}) = 0$, 2 or 4 is

$$1 + \begin{pmatrix} 2^r \\ 2 \end{pmatrix} + \begin{pmatrix} 2^r \\ 4 \end{pmatrix}$$

.

By Lemma 2.1.9 in Section 2.1, the 4-error linear complexity of $s^{(r)} + t^{(r)}$ is c.

By Lemma 2.1.6 and Lemma 2.1.8 in Section 2.1, the number of binary sequences $s^{(r)} + t^{(r)}$ is

$$2^{c-1} \times (1 + \begin{pmatrix} 2^r \\ 2 \end{pmatrix} + \begin{pmatrix} 2^r \\ 4 \end{pmatrix})$$

By Lemma 2.1.5 in Section 2.1, there are $2^{2^{n-1}+\cdots+2^r} = 2^{2^n - 2^r}$ binary sequences $s^{(n)} + t^{(n)}$, such that $s^{(r)} + t^{(r)} = \varphi_{r+1} \cdots \varphi_n(s^{(n)} + t^{(n)})$, $t^{(r)} = \varphi_{r+1} \cdots \varphi_n(t^{(n)})$ and $W_H(t^{(n)}) = W_H(t^{(r)})$. Thus the 4-error linear complexity of $s^{(n)} + t^{(n)}$ is $2^{n-1} + \cdots + 2^r + L_4(s^{(r)} + t^{(r)}) = 2^n - 2^r + c = L(r,c)$. Therefore,

$$N_4(L(r,c)) = 2^{2^n - 2^r} \times 2^{c-1} \times (1 + \begin{pmatrix} 2^r \\ 2 \end{pmatrix} + \begin{pmatrix} 2^r \\ 4 \end{pmatrix}) = 2^{L(r,c)-1}(1 + \begin{pmatrix} 2^r \\ 2 \end{pmatrix} + \begin{pmatrix} 2^r \\ 4 \end{pmatrix})$$

□

Now by summarizing all the results above and using the technique of extending the period from 2^r to 2^n used in Lemma 2.5.7, we can have the main result of this chapter in the following theorem.

Theorem 2.5.1 Let $L(r,c) = 2^n - 2^r + c$, $2 \le r \le n, 1 \le c \le 2^{r-1} - 1$, and $N_4(L)$ be the number of 2^n-periodic binary sequences with the linear complexity less than 2^n and 4-error linear complexity L. Then

$$N_4(L) = \begin{cases} 1 + \binom{2^n}{2} + \binom{2^n}{4}, \\ \qquad L = 0 \\ 2^{L(r,c)-1}(1 + \binom{2^r}{2} + \binom{2^r}{4}), \\ \qquad L = L(r,c), 1 \le c \le 2^{r-3} - 1, r > 3 \\ 2^{L(r,c)-1} f(r,m), \\ \qquad L = L(r,c), c = 2^{r-2} - 2^{r-m}, 2 < m \le r, r > 2 \\ 2^{L(r,c)-1} g(r,m), \\ \qquad L = L(r,c), c = 2^{r-2} - 2^{r-m} + x, 2 < m < r-1, 0 < x < 2^{r-m-1}, r > 4 \\ 2^{L(r,c)-1} h(r,m), \\ \qquad L = L(r,c), c = 2^{r-1} - 2^{r-m}, 2 \le m \le r, r \ge 2 \\ 2^{L(r,c)-1} p(r,m,j), \\ \qquad L = L(r,c), c = 2^{r-1} - (2^{r-m} + 2^{r-j}), 2 < m < j \le r, r > 3 \\ 2^{L(r,c)-1} q(r,m,j), \\ \qquad L = L(r,c), c = 2^{r-1} - (2^{r-m} + 2^{r-j}) + x, \\ \qquad\quad 2 < m < j < r-1, 0 < x < 2^{r-j-1}, r > 5 \\ 0, \qquad \text{otherwise} \end{cases}$$

where $f(r,m)$, $g(r,m)$, $h(r,m)$, $p(r,m,j)$, $q(r,m,j)$ are defined in Lemma 2.5.1, 2.5.2, 2.5.3, 2.5.5 and 2.5.6 respectively.

From Theorem 2.5.1, for $n = 5$, the numbers of 2^n-periodic binary sequences with linear complexity less than 2^n and the 4-error linear complexity c, $0 \le c < 2^n$, are shown in Table 2.2, and these results are also checked by a computer program.

Table 2.2: $N_4(L(r,c))$ by Theorem 2.5.1.

$L(r,c)$	$N_4(L(r,c))$	$L(r,c)$	$N_4(L(r,c))$
0	36457	16	0
1	36457	17	127205376
2	72914	18	236060672
3	145828	19	418643968
4	289416	20	134217728
5	581072	21	567279616
6	1144608	22	33554432
7	2236992	23	16777216
8	2293760	24	0
9	6837504	25	486539264
10	13210112	26	0
11	25031680	27	0
12	14876672	28	0
13	46845952	29	0
14	8978432	30	0
15	4587520	31	0

The summation of numbers in both the second and fourth column of Table 2.2 is 2^{31}.

2.6 Counting functions for the 5-error linear complexity

For a 2^n-periodic binary sequence with *linear complexity* 2^n, the change of 2 or 4 bits in each period results in a sequence with odd number of nonzero bits in the same period, which still has *linear complexity* 2^n. In this section, we thus focus on the number of sequences with the *linear complexity* 2^n and 5-error linear complexity taking different values.

By using the approach of Lemma 2.5.7, we can have the following result on the distribution of the sequences with the *linear complexity of* 2^n and 5-error linear complexity in some range. First we have the following result.

Lemma 2.6.1 Let $L(r,c) = 2^n - 2^r + c, 4 \le r \le n, 1 \le c \le 2^{r-3} - 1$, and $N_5(L)$ be the number of 2^n-periodic binary sequences with the *linear complexity* 2^n and 5-error linear complexity L. Then

$$N_5(L) = \begin{cases} \binom{2^n}{5} + \binom{2^n}{3} + 2^n, & L = 0 \\ 2^{L-1}(\binom{2^r}{5} + \binom{2^r}{3} + 2^r), & L = L(r,c) \end{cases}$$

In order to tackle this problem thoroughly, we only need to consider for the cases with linear complexity $L(r,c) = 2^n - 2^r + c, 4 \le r \le n, 2^{r-3} \le c < 2^{r-1}$. Now by Lemma 2.1.9 in Section 2.1, we only need to consider the following three cases.

i) $c = 2^{n-1} - 2^{d_1} - 2^{d_2}, 0 \le d_2 < d_1 \le n-2$.

ii) $c = 2^{n-1} - 2^{d_1} - 2^{d_2} + x, 0 \le d_2 < d_1 \le n-2, 0 < x < 2^{d_2-1}$.

iii) $c = 2^{n-1} - 2^{d_1}, 0 \le d_1 \le n-2$.

Among all these three cases, the most complicated one is $c = 2^{n-1} - 2^{d_1} - 2^{d_2}, 0 \le d_2 < d_1 \le n-2$. We need to characterize the case that $w^{(n)} = u^{(n)} + v^{(n)}$, with $W(u^{(n)}) = 3$ or 5, $W(v^{(n)}) = 3$ or 5, $L(w^{(n)}) = 2^{n-1} - 2^{d_1} - 2^{d_2}$ and $W(w^{(n)}) = 8$. Nevertheless, we have characterized the case that $w^{(n)} = u^{(n)} + v^{(n)}$, with $W(u^{(n)}) = 4$, $W(v^{(n)}) = 4$, $L(w^{(n)}) = 2^{n-1} - 2^{d_1} - 2^{d_2}$ and $W(w^{(n)}) = 8$ in the previous section. Next in Lemma 2.6.3 we will present a special case with $d_1 = n-2$ in i). Also, $2^{n-1} - 2^{n-3}$ in Lemma 2.6.4 is a special case of iii). We expect the techniques used in these proofs will be useful to solve

this problem completely in future.

First we consider the category of sequences with the 5-error linear complexity $2^{n-3}+x = 2^{n-1}-2^{n-2}-2^{n-3}+x$, which is a special case of ii).

Lemma 2.6.2 Let $N_5(2^{n-3}+x)$ be the number of 2^n-periodic binary sequences with linear complexity 2^n and 5-error linear complexity $2^{n-3}+x, n \geq 5, 1 \leq x < 2^{n-4}$. Then

$$\begin{aligned} & N_5(2^{n-3}+x) \\ = \; & [2^n + \binom{2^n}{3} + \binom{2^n}{5} - 2^{n-3}\binom{8}{3} - 2^{n-4}\binom{8}{4}(2^n-8)] \times 2^{2^{n-3}+x-1} \end{aligned}$$

Proof. Let $S = \{s|L(s) = 2^{n-3}+x\}, E = \{e|W(e) = 1, 3 \text{ or } 5\}, S+E = \{s+e|s \in S, e \in E\}$. By Lemma 2.1.6 in Section 2.1, the number of 2^n-periodic binary sequences with linear complexity $2^{n-3}+x$ is $2^{2^{n-3}+x-1}$. As the number of 2^n-periodic binary sequences in E is $2^n + \binom{2^n}{3} + \binom{2^n}{5}$, so the number of 2^n-periodic binary sequences $s+e \in S+E$ is at most $(2^n + \binom{2^n}{3} + \binom{2^n}{5})2^{2^{n-3}+x-1}$.

We first characterize the set $LESS$. Suppose that $w^{(n)} = u^{(n)} + v^{(n)}$, with $W(u^{(n)}) = 1, 3$ or 5, $W(v^{(n)}) = 1, 3$ or 5, and $L(w^{(n)}) \leq 2^{n-3}+x$. As $1 \leq x < 2^{n-4}$, thus $L(w^{(n)}) \leq 2^{n-3}+x < 2^{n-2}$. Therefore, $w^{(n)}$ can be divided into 4 equal parts with $W(w^{(n)}) = 8$. So, $L(w^{(n)}) = 2^{n-2} - 2^{n-m}, 3 \leq m \leq n$.

If $m = 3$, then $L(w^{(n)}) = 2^{n-3}$. The number of these $w^{(n)}$ is 2^{n-3}.

If $m > 3$, then $L(w^{(n)}) = 2^{n-2} - 2^{n-m} \geq 2^{n-2} - 2^{n-4} = 2^{n-3} + 2^{n-4} > 2^{n-3} + x$. This contradicts the condition that $L(w^{(n)}) \leq 2^{n-3}+x$. Thus m can only be 3.

As $L(u^{(n)}+v^{(n)})$ can only be 2^{n-3}, thus the case that $s+e \in S+E$ but $L_5(s+e) < 2^{n-3}+x$ does not exist. Namely, $LESS$ is empty.

Second we characterize the set $EQUAL$ by dividing the $u^{(n)} + v^{(n)}$ with $L(u^{(n)} + v^{(n)}) = 2^{n-3}$ into 3 cases.

Case 1): $W(u^{(n)}) = 3$, there exists exactly one $v^{(n)}$ with $W(v^{(n)}) = 5$, such that $L(u^{(n)} +$

$v^{(n)}) = 2^{n-3}$. In this case, the number of these $u^{(n)}$ can be given by

$$A1 = 2^{n-3} \left(\begin{array}{c} 8 \\ 3 \end{array} \right).$$

Case 2): $W(u^{(n)}) = 5$ and all 5 nonzero elements of $u^{(n)}$ are in $w^{(n)}$, there exists exactly one $v^{(n)}$ with $W(v^{(n)}) = 3$, such that $L(u^{(n)} + v^{(n)}) = 2^{n-3}$. In this case, the number of these $u^{(n)}$ can be given by

$$A2 = 2^{n-3} \left(\begin{array}{c} 8 \\ 5 \end{array} \right).$$

Case 3): $W(u^{(n)}) = 5$ and only 4 nonzero elements of $u^{(n)}$ are in $w^{(n)}$, there exists exactly one $v^{(n)}$ with $W(v^{(n)}) = 5$, such that $L(u^{(n)} + v^{(n)}) = 2^{n-3}$. The number of these $u^{(n)}$ can be given by

$$A3 = 2^{n-3} \left(\begin{array}{c} 8 \\ 4 \end{array} \right) (2^n - 8).$$

We have that the number of sequences in $EQUAL$ is $A1 + A2 + A3$, which leads to the following

$$\begin{aligned} & N_5(2^{n-3} + x) \\ = \; & [2^n + \left(\begin{array}{c} 2^n \\ 3 \end{array} \right) + \left(\begin{array}{c} 2^n \\ 5 \end{array} \right) - \frac{1}{2}A1 - \frac{1}{2}A2 - \frac{1}{2}A3]2^{2^{n-3}+x-1} \\ = \; & [2^n + \left(\begin{array}{c} 2^n \\ 3 \end{array} \right) + \left(\begin{array}{c} 2^n \\ 5 \end{array} \right) - 2^{n-3} \left(\begin{array}{c} 8 \\ 3 \end{array} \right) - 2^{n-4} \left(\begin{array}{c} 8 \\ 4 \end{array} \right) (2^n - 8)]2^{2^{n-3}+x-1} \end{aligned}$$

This completes the proof. □

As a simple illustrative example, let $n = 5, x = 1$. Then $2^{n-3} + x = 5$, $N_5(2^{n-3} + x) = 3244544$, which can be easily verified by a computer program.

Next we consider the category of sequences with the 5-error linear complexity $2^{n-2} - 2^{n-m}$, which is a special case of i).

Lemma 2.6.3 Let $N_5(2^{n-2} - 2^{n-m})$ be the number of 2^n-periodic binary sequences with

linear complexity 2^n and 5-error linear complexity $2^{n-2}-2^{n-m}, n \geq 4, 4 \leq m \leq n$. Then

$$\begin{aligned} & N_5(2^{n-2}-2^{n-m}) \\ = \; & [2^n + \left(\begin{array}{c} 2^n \\ 3 \end{array} \right) + \left(\begin{array}{c} 2^n \\ 5 \end{array} \right) - B1 - B2 - B3 \\ & -\frac{1}{2}B4 - \frac{1}{2}B5 - \frac{1}{2}B6 - \frac{2}{3}B7] \times 2^{2^{n-2}-2^{n-m}-1} \end{aligned}$$

where $B1, B2, B3, B4, B5, B6, B7$ are defined in the following proof.

Proof. Let

$$S = \{s|L(s) = 2^{n-2}-2^{n-m}\}, E = \{e|W(e) = 1, 3 \text{ or } 5\}$$

$$S + E = \{s + e|s \in S, e \in E\}$$

.

As the number of 2^n-periodic binary sequences in E is $2^n + \left(\begin{array}{c} 2^n \\ 3 \end{array} \right) + \left(\begin{array}{c} 2^n \\ 5 \end{array} \right)$, the number of 2^n-periodic binary sequences $s + e \in S + E$ is at most

$$(2^n + \left(\begin{array}{c} 2^n \\ 3 \end{array} \right) + \left(\begin{array}{c} 2^n \\ 5 \end{array} \right))2^{2^{n-2}-2^{n-m}-1}$$

.

We first characterize the set $LESS$.

Case 1): Suppose that $w^{(n)} = u^{(n)} + v^{(n)}$ with $W(u^{(n)}) = 1, 3$ or 5, $W(v^{(n)}) = 1, 3$ or 5. By Lemma 2.1.9 in Section 2.1, there exists $w^{(n)}$ such that $L(w^{(n)}) = 2^{n-2}-2^{n-m}$. So $L_5(s + u^{(n)}) < 2^{n-2}-2^{n-m}$. Then one can show that $W(w^{(n)}) = 8$, and $w^{(n)}$ can be divided into 4 equal parts. Each part has exactly 2 nonzero elements with a distance $2^{n-m}(2i+1)$. The number of these $w^{(n)}$ is

$$(2^{n-2}-2^{n-m}) + (2^{n-2}-2^{n-m} \times 3) + \cdots + [2^{n-2}-2^{n-m} \times (\frac{2^{n-2}}{2^{n-m}} - 1)] = 2^{n+m-6}.$$

Each of these $w^{(n)}$ and other $2(\frac{2^{n-2}}{2 \times 2^{n-m}} - 1) = 2(2^{m-3} - 1)$ distinct $w^{(n)}$ have the intersection of 4 nonzero elements, which constitute the set $P = \{a_i, a_{i+2^{n-2}}, a_{i+2^{n-1}}, a_{i+3 \times 2^{n-2}} | 0 \leq i < 2^{n-2}\}$. Thus the size of set P is 2^{n-2}. Now we only need to consider the following three cases.

Case 1.1): Suppose that $w^{(n)} = u^{(n)} + v^{(n)}$, where $L(w^{(n)}) = 2^{n-2}-2^{n-m}$, $W(w^{(n)}) = 8$, $W(u^{(n)}) = 3$, $W(v^{(n)}) = 5$.

If 3 nonzero elements of $u^{(n)}$ are contained in $\{a_i, a_{i+2^{n-2}}, a_{i+2^{n-1}}, a_{i+3\times 2^{n-2}}\}$, $0 \le i < 2^{n-2}\}$, then the number of these $u^{(n)}$ is $2^{n-2}\begin{pmatrix} 4 \\ 3 \end{pmatrix}$. Thus the number of other $u^{(n)}$ is $2^{n+m-6}[\begin{pmatrix} 8 \\ 3 \end{pmatrix} - 2\begin{pmatrix} 4 \\ 3 \end{pmatrix}]$.

In this case, the total number of $u^{(n)}$ is $B1 = 2^{n+m-6}[\begin{pmatrix} 8 \\ 3 \end{pmatrix} - 2\begin{pmatrix} 4 \\ 3 \end{pmatrix}] + 2^{n-2}\begin{pmatrix} 4 \\ 3 \end{pmatrix}$

Case 1.2): Suppose that $w^{(n)} = u^{(n)} + v^{(n)}$, where $L(w^{(n)}) = 2^{n-2} - 2^{n-m}$, $W(w^{(n)}) = 8$, $W(u^{(n)}) = 5$, $W(v^{(n)}) = 3$. In this case, the total number of $u^{(n)}$ is $B2 = 2^{n+m-6}\begin{pmatrix} 8 \\ 5 \end{pmatrix}$

Case 1.3): Suppose that $w^{(n)} = u^{(n)} + v^{(n)}$, where $L(w^{(n)}) = 2^{n-2} - 2^{n-m}$, $W(w^{(n)}) = 8$, $W(u^{(n)}) = 5$, $W(v^{(n)}) = 5$.

Case 1.3.1): If 4 nonzero elements of $u^{(n)}$ are $\{a_i, a_{i+2^{n-2}}, a_{i+2^{n-1}}, a_{i+3\times 2^{n-2}}\}$, $0 \le i < 2^{n-2}$, then the distance of the fifth nonzero element of $u^{(n)}$ and a_i can not be $2^{n-m}(2j+1), j \ge 0$. Otherwise, $u^{(n)}$ is in the case of (1.2).

Suppose that the distance of the fifth nonzero element of $u^{(n)}$ and a_i is not $2^{n-m}(2j+1), j \ge 0$, then the number of possible location of the fifth nonzero element of $u^{(n)}$ is $2^n - \frac{2^{n-2}}{2^{n-m}\times 2} \times 4 - 4 = 2^n - 2^{m-1} - 4$. Thus the total number of $u^{(n)}$ in this case is $2^{n-2}(2^n - 2^{m-1} - 4)$.

Case 1.3.2): If there are no 4 nonzero elements in $u^{(n)}$, which are $\{a_i, a_{i+2^{n-2}}, a_{i+2^{n-1}}, a_{i+3\times 2^{n-2}}\}$, $0 \le i < 2^{n-2}$, then the number of $u^{(n)}$ in this case is $2^{n+m-6}[\begin{pmatrix} 8 \\ 4 \end{pmatrix} - 2](2^n - 8)$.

The following case must be noted. Suppose that 5 nonzero elements of $u^{(n)}$ are b_1, b_2, b_3, b_4, b_5, and $b_1, b_2, b_3 \subset \{a_i, a_{i+2^{n-2}}, a_{i+2^{n-1}}, a_{i+3\times 2^{n-2}}\}$, $0 \le i < 2^{n-2}$,
$d(b_4, a_i) = 2^{n-m}(2j_1+1), j_1 \ge 0$, $d(b_5, a_i) = 2^{n-m}(2j_2+1), j_2 \ge 0$, but $d(b_4, b_5)$ is not the multiple of 2^{n-2}. In this case, we can obtain two different $w^{(n)}$ with the same $u^{(n)}$. The number of $u^{(n)}$ in this case is

$$2^{n-2}\begin{pmatrix} 4 \\ 3 \end{pmatrix}\begin{pmatrix} 2^{m-3} \\ 2 \end{pmatrix}\begin{pmatrix} 4 \\ 1 \end{pmatrix}\begin{pmatrix} 4 \\ 1 \end{pmatrix} = 2^{n+4}\begin{pmatrix} 2^{m-3} \\ 2 \end{pmatrix}.$$

Therefore, in the case of $W(u^{(n)}) = 5$ and $W(v^{(n)}) = 5$, the total number of $u^{(n)}$ is

$$B3 = 2^{n-2}(2^n - 2^{m-1} - 4) + 2^{n+m-6}[\begin{pmatrix} 8 \\ 4 \end{pmatrix} - 2](2^n - 8) - 2^{n+4}\begin{pmatrix} 2^{m-3} \\ 2 \end{pmatrix}.$$

Second we characterize the set $EQUAL$.

Case 2): Let $w^{(n)} = u^{(n)} + v^{(n)}$ with $L(u^{(n)} + v^{(n)}) = 2^{n-2} - 2^{n-k}$, $3 \leq k < m$.

Let $P_k = \{w^{(n)} | L(w^{(n)}) = 2^{n-2} - 2^{n-k}, 3 \leq k < m\}$. Then the size of set P_k is 2^{n+k-6}.

Case 2.1): Suppose that $w^{(n)} = u^{(n)} + v^{(n)}$, where $L(w^{(n)}) = 2^{n-2} - 2^{n-k}$, $W(w^{(n)}) = 8$, $W(u^{(n)}) = 3$, $W(v^{(n)}) = 5$, and the 3 nonzero elements of $u^{(n)}$ are not contained in an element of set P. In this case, the total number of such $u^{(n)}$ is

$$B4 = \sum_{k=3}^{m-1} 2^{n+k-6}[\begin{pmatrix} 8 \\ 3 \end{pmatrix} - 2\begin{pmatrix} 4 \\ 3 \end{pmatrix}] = 48(2^{n+m-7} - 2^{n-3}).$$

Case 2.2.1): Suppose that $w^{(n)} = u^{(n)} + v^{(n)}$, where $L(w^{(n)}) = 2^{n-2} - 2^{n-k}$, $W(w^{(n)}) = 8$, $W(u^{(n)}) = 5$, $W(v^{(n)}) = 3$, and the 4 nonzero elements of $u^{(n)}$ are b_1, b_2, b_3, b_4, which are contained in one element of set P. The distance of the fifth element of $u^{(n)}$ and b_1 is $2^{n-k}(2j+1)$, which is an even multiple of 2^{n-m}. In this case, $u^{(n)}$ is in fact in the case of (1.3.1).

Case 2.2.2): Suppose that $w^{(n)} = u^{(n)} + v^{(n)}$, where $L(w^{(n)}) = 2^{n-2} - 2^{n-k}$, $W(w^{(n)}) = 8$, $W(u^{(n)}) = 5$, $W(v^{(n)}) = 3$, and there are no 4 nonzero elements of $u^{(n)}$ contained in one element of set P. Thus $u^{(n)}$ is equivalent to the $v^{(n)}$ in the case of (2.1). In this case, the total number of $u^{(n)}$ is $B5 = B4$.

Case 2.3): Suppose that $w^{(n)} = u^{(n)} + v^{(n)}$, where $L(w^{(n)}) = 2^{n-2} - 2^{n-k}$, $W(w^{(n)}) = 8$, $W(u^{(n)}) = 5$, $W(v^{(n)}) = 5$. Let b_1, b_2, b_3, b_4 be the 4 nonzero elements of $u^{(n)}$ contained in $w^{(n)}$. If b_1, b_2, b_3, b_4 are contained in one element of set P, then $u^{(n)}$ is in the case of (1.2) or (1.3.1). Thus the number of remaining $u^{(n)}$ is $2^{n+k-6}[\begin{pmatrix} 8 \\ 4 \end{pmatrix} - 2](2^n - 8)$.

We have to further consider the following special cases.

Case 2.3.1.1): Suppose that b_1, b_2, b_3 are contained in one element of set P, $d(b_1, b_4)$ is an odd multiple of 2^{n-k} and $d(b_1, b_5)$ is an odd multiple of 2^{n-m}. Then $u^{(n)}$ is in the case of

(1.3.2). In this case, the total number of $u^{(n)}$ is

$$2^{n-2}\begin{pmatrix} 4 \\ 3 \end{pmatrix}\begin{pmatrix} 2^{k-1} \\ 1 \end{pmatrix}\begin{pmatrix} 2^{m-1} \\ 1 \end{pmatrix} = 2^n\begin{pmatrix} 2^{k-1} \\ 1 \end{pmatrix}\begin{pmatrix} 2^{m-1} \\ 1 \end{pmatrix}.$$

Case 2.3.1.2): Suppose that b_1, b_2, b_3 are contained in one element of set P, $d(b_1, b_4)$ is an odd multiple of 2^{n-k} and $d(b_1, b_5)$ is an odd multiple of $2^{n-j}, k < j < m$. Then there exist 2 distinct $v^{(n)}$ with $W(v^{(n)}) = 5$, such that $L(u^{(n)} + v^{(n)}) < 2^{n-2} - 2^{n-m}$. In this case, the total number of $u^{(n)}$ is $2^n\begin{pmatrix} 2^{k-1} \\ 1 \end{pmatrix}\begin{pmatrix} 2^{j-1} \\ 1 \end{pmatrix}$.

Similarly, if $d(b_1, b_4)$ is an odd multiple of 2^{n-k} and $d(b_1, b_5)$ is also an odd multiple of $2^{n-k}, 4 \leq k < m$, and $d(b_4, b_5)$ is not a multiple of 2^{n-2}, then there exist 2 distinct $v^{(n)}$ with $W(v^{(n)}) = 5$, such that $L(u^{(n)} + v^{(n)}) < 2^{n-2} - 2^{n-m}$. In this case, the total number of $u^{(n)}$ is $2^{n+4}\begin{pmatrix} 2^{k-3} \\ 2 \end{pmatrix}$.

We will consider these two cases in case 2.3.2) again later. In these two cases, we can obtain two different $w^{(n)}$ with the same $u^{(n)}$.

Therefore, the total number of $u^{(n)}$ here is

$$\begin{aligned} B6 \;=\; & \sum_{k=3}^{m-1}\{2^{n+k-6}[\begin{pmatrix} 8 \\ 4 \end{pmatrix} - 2](2^n - 8) - 2^n\begin{pmatrix} 2^{k-1} \\ 1 \end{pmatrix}\begin{pmatrix} 2^{m-1} \\ 1 \end{pmatrix} \\ & - \sum_{j=k+1}^{m-1} 2 \times 2^n\begin{pmatrix} 2^{k-1} \\ 1 \end{pmatrix}\begin{pmatrix} 2^{j-1} \\ 1 \end{pmatrix}\} - \sum_{k=4}^{m-1} 2 \times 2^{n+4}\begin{pmatrix} 2^{k-3} \\ 2 \end{pmatrix} \end{aligned}$$

For each $u^{(n)}$ here, there exists exactly one $v^{(n)}$ with $W(v^{(n)}) = 5$, such that $L(u^{(n)}+v^{(n)}) < 2^{n-2} - 2^{n-m}$. So $u^{(n)}$ is in $EQUAL$.

Case 2.3.2): Now we consider the two cases for case 2.3.1).

Suppose that b_1, b_2, b_3 are contained in one element of set P, $d(b_1, b_4)$ is an odd multiple of 2^{n-k} and $d(b_1, b_5)$ is an odd multiple of $2^{n-j}, k < j < m$. Then there exist $v_1^{(n)}$, $v_2^{(n)}$ with $v_1^{(n)} \neq v_2^{(n)}$, $W(v_1^{(n)}) = W(v_2^{(n)}) = 5$, such that $L(u^{(n)}+v_1^{(n)}) = 2^{n-2}-2^{n-k} < 2^{n-2}-2^{n-m}$, $L(u^{(n)} + v_2^{(n)}) = 2^{n-2} - 2^{n-j} < 2^{n-2} - 2^{n-m}$.

Similarly, if $d(b_1, b_4)$ is an odd multiple of 2^{n-k} and $d(b_1, b_5)$ is also an odd multiple of $2^{n-k}, 4 \leq k < m$, and $d(b_4, b_5)$ is not a multiple of 2^{n-2}, then there exist $v_1^{(n)}$, $v_2^{(n)}$

with $v_1^{(n)} \neq v_2^{(n)}$, $W(v_1^{(n)}) = W(v_2^{(n)}) = 5$, such that $L(u^{(n)} + v_1^{(n)}) = L(u^{(n)} + v_2^{(n)}) = 2^{n-2} - 2^{n-k} < 2^{n-2} - 2^{n-m}$.So $u^{(n)}$ is in $EQUAL$. Suppose that all $u^{(n)}$ here form a set U. Then the size of U is

$$B7 = \sum_{k=3}^{m-2} \sum_{j=k+1}^{m-1} 2^n \begin{pmatrix} 2^{k-1} \\ 1 \end{pmatrix} \begin{pmatrix} 2^{j-1} \\ 1 \end{pmatrix} + \sum_{k=4}^{m-1} 2^{n+4} \begin{pmatrix} 2^{k-3} \\ 2 \end{pmatrix}$$

(For easy understanding, the following special case with $n = m = 6$ is given to illustrate the construction of $v^{(n)}$. For $n = m = 6$, k could be $3, 4, 5$. Let b_1, b_2, b_3, b_4, b_5 be the 5 nonzero elements of $u^{(n)}$, and b_1, b_2, b_3 are contained in one element of set P. Let

$$\begin{aligned} Q_{2,2} &= \{u^{(n)} | d(b_1, b_4) \text{ is an odd multiple of } 2 = 2^{n-5}, \\ &\quad d(b_1, b_5) \text{ is an odd multiple of } 2 = 2^{n-5}, \\ &\quad d(b_4, b_5) \text{ is not a multiple of } 2^{n-2}\} \end{aligned}$$

$$\begin{aligned} Q_{2,8} &= \{u^{(n)} | d(b_1, b_4) \text{ is an odd multiple of } 2 = 2^{n-5}, \\ &\quad d(b_1, b_5) \text{ is an odd multiple of } 2^3 = 2^{n-3}\} \end{aligned}$$

$$\begin{aligned} Q_{2,4} &= \{u^{(n)} | d(b_1, b_4) \text{ is an odd multiple of } 2 = 2^{n-5}, \\ &\quad d(b_1, b_5) \text{ is an odd multiple of } 2^2 = 2^{n-4}\} \end{aligned}$$

(i). For $u^{(n)} \in Q_{2,2}$, there exist $v_1^{(n)}$, $v_2^{(n)}$ with $v_1^{(n)} \neq v_2^{(n)}$, $W(v_1^{(n)}) = W(v_2^{(n)}) = 5$, such that $L(u^{(n)} + v_1^{(n)}) = L(u^{(n)} + v_2^{(n)}) = 2^{n-2} - 2 < 2^{n-2} - 2^{n-m}$. $d(b_4, b_5)$ could be 4 or 8.

If $d(b_4, b_5) = 4$, then both $v_1^{(n)}$, $v_2^{(n)}$ are in $Q_{2,4}$. If $d(b_4, b_5) = 8$, then both $v_1^{(n)}$, $v_2^{(n)}$ are in $Q_{2,8}$.

(ii). For $u^{(n)} \in Q_{2,8}$, there exist $v_1^{'(n)}$, $v_2^{'(n)}$ with $v_1^{'(n)} \neq v_2^{'(n)}$, $W(v_1^{'(n)}) = W(v_2^{'(n)}) = 5$, such that $L(u^{(n)} + v_1^{'(n)}) = 2^{n-2} - 2 < 2^{n-2} - 2^{n-m}$, $L(u^{(n)} + v_2^{'(n)}) = 2^{n-2} - 8 < 2^{n-2} - 2^{n-m}$. So $v_1^{'(n)} \in Q_{2,2}$, $v_2^{'(n)} \in Q_{2,8}$.

(iii). For $u^{(n)} \in Q_{2,4}$, there exist $v_1^{''(n)}$, $v_2^{''(n)}$ with $v_1^{''(n)} \neq v_2^{''(n)}$, $W(v_1^{''(n)}) = W(v_2^{''(n)}) = 5$, such that $L(u^{(n)} + v_1^{''(n)}) = 2^{n-2} - 2 < 2^{n-2} - 2^{n-m}$, $L(u^{(n)} + v_2^{''(n)}) = 2^{n-2} - 4 < 2^{n-2} - 2^{n-m}$. So $v_1^{''(n)} \in Q_{2,2}$, $v_2^{''(n)} \in Q_{2,4}$.

In summary, all $v_1^{(n)}$, $v_2^{(n)}$, $v_1^{'(n)}$, $v_2^{'(n)}$, $v_1^{''(n)}$, $v_2^{''(n)}$ are in $Q_{2,2}$, $Q_{2,4}$, $Q_{2,8}$, respectively.)

It follows that

$$\begin{aligned} & N_5(2^{n-2}-2^{n-m}) \\ = \; & [2^n + \begin{pmatrix} 2^n \\ 3 \end{pmatrix} + \begin{pmatrix} 2^n \\ 5 \end{pmatrix} - B1 - B2 - B3 - \frac{1}{2}B4 \\ & -\frac{1}{2}B5 - \frac{1}{2}B6 - \frac{2}{3}B7] \times 2^{2^{n-2}-2^{n-m}-1} \end{aligned}$$

□

As an illustrative example, let $n = m = 5$. Then $2^{n-2} - 2^{n-m} = 7$, $N_5(2^{n-2} - 2^{n-m}) = 11184128$, which is verified by simulation.

Finally we consider the category of sequences with the 5-error linear complexity $2^{n-1} - 2^{n-3}$, which is a special case of iii).

Lemma 2.6.4 Let $N_5(2^{n-1} - 2^{n-3})$ be the number of 2^n-periodic binary sequences with the linear complexity 2^n and 5-error linear complexity $2^{n-1} - 2^{n-3}, n \geq 5$. Then

$$N_5(2^{n-1} - 2^{n-3}) = [\begin{pmatrix} 2^n \\ 5 \end{pmatrix} - C1 - C2 + \frac{1}{4}C3 - C4 + \frac{1}{2}C5] \times 2^{2^{n-1}-2^{n-3}-1}$$

where $C1, C2, C3, C4, C5$ are defined in the following proof.

Proof. As the number of 2^n-periodic binary sequences in E is $2^n + \begin{pmatrix} 2^n \\ 3 \end{pmatrix} + \begin{pmatrix} 2^n \\ 5 \end{pmatrix}$, the number of 2^n-periodic binary sequences $s + e \in S + E$ is at most

$$(2^n + \begin{pmatrix} 2^n \\ 3 \end{pmatrix} + \begin{pmatrix} 2^n \\ 5 \end{pmatrix})2^{2^{n-1}-2^{n-3}-1}.$$

First we consider the case that $W(u^{(n)}) = 1$ or 3. There exists a $v^{(n)}$ with $W(v^{(n)}) = 3$ or 5, such that $L(u^{(n)} + v^{(n)}) = 2^{n-1} - 2^{n-3}$. So $u^{(n)}$ is in $LESS$.

Second we consider the case of $W(u^{(n)}) = 5$. Let us divide one period of $u^{(n)}$ into 2^{n-3} subsequences with the following form

$$\{(u_a, u_{a+2^{n-3}}, u_{a+2^{n-3}+1}, \cdots, u_{a+7\times 2^{n-3}}) | 0 \leq a < 2^{n-3}\}$$

Case 1): Suppose that there are at least 3 nonzero elements of $u^{(n)}$ contained in one subsequence. Then there exists a $v^{(n)}$ with $W(v^{(n)}) = 1$, 3 or 5, such that $L(u^{(n)} + v^{(n)}) = 2^{n-1} - 2^{n-3}$. So $u^{(n)}$ is in $LESS$.

Assume that there are 5 nonzero element of $u^{(n)}$ contained in one subsequence. Then the number of these $u^{(n)}$ is $2^{n-3}\begin{pmatrix} 8 \\ 5 \end{pmatrix}$.

Suppose that there are 4 nonzero element of $u^{(n)}$ contained in one subsequence. Then the number of these $u^{(n)}$ is $6\begin{pmatrix} 2^{n-3} \\ 2 \end{pmatrix}\begin{pmatrix} 8 \\ 4 \end{pmatrix}$.

Assume that there are 3 nonzero element of $u^{(n)}$ contained in one subsequence and the other 2 nonzero elements of $u^{(n)}$ contained in another subsequence. Then the number of these $u^{(n)}$ is

$$2\begin{pmatrix} 2^{n-3} \\ 2 \end{pmatrix}\begin{pmatrix} 8 \\ 3 \end{pmatrix}\begin{pmatrix} 8 \\ 2 \end{pmatrix}$$

Suppose that there are 3 nonzero elements of $u^{(n)}$ contained in one subsequence and the other 2 nonzero elements of $u^{(n)}$ contained in two subsequences respectively. Then the number of these $u^{(n)}$ is $192\begin{pmatrix} 2^{n-3} \\ 3 \end{pmatrix}\begin{pmatrix} 8 \\ 3 \end{pmatrix}$.

The total number of these $u^{(n)}$ is

$$C1 = 2^{n-3}\begin{pmatrix} 8 \\ 5 \end{pmatrix}+16\begin{pmatrix} 2^{n-3} \\ 2 \end{pmatrix}\begin{pmatrix} 8 \\ 4 \end{pmatrix}+2\begin{pmatrix} 2^{n-3} \\ 2 \end{pmatrix}\begin{pmatrix} 8 \\ 3 \end{pmatrix}\begin{pmatrix} 8 \\ 2 \end{pmatrix}+192\begin{pmatrix} 2^{n-3} \\ 3 \end{pmatrix}\begin{pmatrix} 8 \\ 3 \end{pmatrix}$$

For each of these $u^{(n)}$, there exists a $v^{(n)}$ with $W(v^{(n)}) = 5$, such that $L(u^{(n)} + v^{(n)}) = 2^{n-1} - 2^{n-3}$.

Case 2): Suppose that there are 2 nonzero elements b_1, b_2 of $u^{(n)}$ contained in one subsequence and the other 2 nonzero elements b_3, b_4 of $u^{(n)}$ contained in another subsequence, and the final nonzero element of $u^{(n)}$ contained in the third subsequence. Then the number of these $u^{(n)}$ is

$$C2 = 24\begin{pmatrix} 2^{n-3} \\ 3 \end{pmatrix}\begin{pmatrix} 8 \\ 2 \end{pmatrix}^2$$

We now consider $u^{(n)}$ with $d(b_1, b_2)$ is an even multiple of 2^{n-3} and $d(b_3, b_4)$ is an even multiple of 2^{n-3}, but neither $d(b_1, b_2)$ nor $d(b_3, b_4)$ is 2^{n-1}. The number of these $u^{(n)}$ is $C3 = 3 \times 2^9\begin{pmatrix} 2^{n-3} \\ 3 \end{pmatrix}$.

For each $u^{(n)}$ of this kind, there exist $v_1^{(n)}$, $v_2^{(n)}$ and $v_3^{(n)}$ with $W(v_1^{(n)}) = W(v_2^{(n)}) = W(v_3^{(n)}) = 5$, such that $L(u^{(n)} + v_1^{(n)}) = L(u^{(n)} + v_2^{(n)}) = 2^{n-2}$, $L(u^{(n)} + v_3^{(n)}) < 2^{n-2}$. So $u^{(n)}$ is in $EQUAL$. For each $u^{(n)}$ of other kinds, there exists a $v^{(n)}$ with $W(v^{(n)}) = 5$, such that $L(u^{(n)} + v^{(n)}) = 2^{n-1} - 2^{n-3}$.

Case 3): Suppose that there are 2 nonzero elements b_1, b_2 of $u^{(n)}$ contained in one subsequence and the other 3 nonzero elements of $u^{(n)}$ contained in 3 distinct subsequences. Then the number of these $u^{(n)}$ is

$$C4 = 2^{11} \left(\begin{array}{c} 2^{n-3} \\ 4 \end{array} \right) \left(\begin{array}{c} 8 \\ 2 \end{array} \right).$$

We now consider $u^{(n)}$ with $d(b_1, b_2) = 2^{n-2}$. The number of these $u^{(n)}$ is $C5 = 2^{14} \left(\begin{array}{c} 2^{n-3} \\ 4 \end{array} \right)$.

For each $u^{(n)}$ of this kind, one can construct exactly one $v^{(n)}$ with $W(v^{(n)}) = 5$, such that $L(u^{(n)} + v^{(n)}) = 2^{n-2}$. So $u^{(n)}$ is in $EQUAL$. For each $u^{(n)}$ of other kinds, there exists a $v^{(n)}$ with $W(v^{(n)}) = 5$, such that $L(u^{(n)} + v^{(n)}) = 2^{n-1} - 2^{n-3}$.

It follows that,

$$\begin{aligned} & N_5(2^{n-1} - 2^{n-3}) \\ = \; & [\left(\begin{array}{c} 2^n \\ 5 \end{array} \right) - C1 - (C2 - C3) - \frac{3}{4}C3 - (C4 - C5) - \frac{1}{2}C5]2^{2^{n-1}-2^{n-3}-1} \\ = \; & [\left(\begin{array}{c} 2^n \\ 5 \end{array} \right) - C1 - C2 + \frac{1}{4}C3 - C4 + \frac{1}{2}C5]2^{2^{n-1}-2^{n-3}-1} \end{aligned}$$

□

As a simple example, let $n = 5$. Then $2^{n-1} - 2^{n-3} = 12$, $N_5(2^{n-1} - 2^{n-3}) = 19922944$, which can be verified by a computer program.

2.7 Complete Characterization of the First Descent Point Distribution for k-error Linear Complexity

In this section, we first derive the counting formula of binary sequences with the same linear complexity and minimum Hamming weight. This result is first obtained in Zhou *et al.* (2013).

Theorem 2.7.1 The number of binary sequences s with period 2^n, $W_H(s) = 2^m$, and $L(s) = 2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m})$, where $0 \le i_1 < i_2 < \cdots < i_m < n$, is

$$2^{2^m n - (2^{m-1} i_m + \cdots + 2i_2 + i_1) - 2^{m+1} + 2}.$$

Proof. The approach to constructing a 2^n-periodic binary sequence $s^{(n)}$ is based on the reverse process of Games-Chan algorithm (Games and Chan, 1983). First we construct sequences with a small period and count the number of these sequences. Second double the period recursively and get the desired sequences, and count the number of all these sequences.

The number of 2^{i_1}-periodic binary sequences $s^{(i_1)}$ with linear complexity 2^{i_1} and $W_H(s^{(i_1)}) = 1$ 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}, where $Left(s^{(i_1+1)}) = Right(s^{(i_1+1)})$.

For $i_2 > i_1$, we aim to obtain 2^{i_2}-periodic binary sequences s^{i_2} with linear complexity $2^{i_2} - 2^{i_1}$ and $W_H(s^{(i_2)}) = 2$ from above 2^{i_1+1}-periodic binary sequences $s^{(i_1+1)}$. In this case, when the sequence period changes from 2^{i_1+1} to 2^{i_2}, the increase of linear complexity is $2^{i_2} - 2^{i_1} - (2^{i_1+1} - 2^{i_1}) = 2^{i_2-1} + 2^{i_2-2} + \cdots + 2^{i_1+1}$.

Based on Step 2 in Algorithm 2.1.1 in Section 2.1, the number of these $s^{(i_2)}$ can be given by $(2^2)^{i_2-i_1-1} \times 2^{i_1} = 2^{2i_2-i_1-2}$. The formula can be easily verified for $i_2 = i_1 + 1$, $i_2 = i_1 + 2$, $i_2 = i_1 + 3$, $\cdots$, respectively.

Next based on Step 1 of Algorithm 2.1.1 in Section 2.1, 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 $2^{2i_2-i_1-2}$.

Similarly for $i_3 > i_2$, the number of 2^{i_3}-periodic binary sequences s^{i_3} with linear complexity

$2^{i_3}-(2^{i_2}+2^{i_1})$ and $W_H(s^{(i_3)})=4$ can be given by $(2^4)^{i_3-i_2-1}\times 2^{2i_2-i_1-2}=2^{4i_3-2i_2-i_1-2-4}$.

.....

Consequently, 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 $W_H(s^{(i_m+1)})=2^m$ is also $2^{2^{m-1}i_m-\cdots-2i_2-i_1-2-4-\cdots-2^{m-1}}$.

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

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

This completes the proof. □

In fact, Etzion *et al.* (2009) proved Theorem 3 in their paper, which is equivalent to Theorem 2.7.1, with a much different approach.

In Theorem 2.7.1, we give the number of sequences with given linear complexity and Hamming weight. Next we will investigate the linear complexity for the sum of two sequences and this will pave the way for our main results in Theorems 2.7.3 and 2.7.4.

Theorem 2.7.2 Suppose that $u^{(n)}, v^{(n)}$ are distinct 2^n-periodic binary sequences with the same linear complexity $2^n-(2^{i_1}+2^{i_2}+\cdots+2^{i_m})$ and $W_H(u^{(n)})=W_H(v^{(n)})=2^m$, where $0\le i_1<i_2<\cdots<i_m<n$. Then $L(u^{(n)}+v^{(n)})=2^n-(\epsilon_m 2^{i_m}+\epsilon_{m-1}2^{i_{m-1}}+\cdots+\epsilon_1 2^{i_1}+2^r)$, where $r\in\{n-1,n-2,\cdots\cdots,1,0\}\setminus\{i_1,i_2,\cdots,i_m\}$ and $\epsilon_1,\epsilon_2,\cdots,\epsilon_m\in\{0,1\}$.

Proof. First we note that two 2^n-periodic binary sequences with the same linear complexity must have the same linear complexity representation $2^n-(2^{i_1}+2^{i_2}+\cdots+2^{i_m})$.

From the proof of Theorem 2.7.1, one can see that $u^{(n)}$ is constructed from $u^{(i_1)}$, $u^{(i_2)},\cdots$, $u^{(i_m)}\cdots$, and $v^{(n)}$ is constructed from $v^{(i_1)}$, $v^{(i_2)},\cdots,v^{(i_m)},\cdots$.

Suppose we use the reverse process of Algorithm 2.1.1 in Section 2.1 to construct a sequence. If the previous period is in $\{i_1,i_2,\cdots,i_m\}$, one doubles the period of a sequence using Step 1 of Algorithm 2.1.1. In this case, we copy the previous sequence to the right

half of the new sequence, so that the right half is the same as the left half of the new sequence. The number of nonzero elements is doubled.

If the previous period is not in $\{i_1, i_2, \cdots, i_m\}$, then we can use the Step 2 of Algorithm 2.1.1 to double the sequence. In this case, every nonzero element of the previous sequence may not move, or move a distance of the previous period. The number of nonzero elements is unchanged.

(For example, suppose that $i_1 = 1, i_2 = 3$, then we have $(2^2)^{i_2 - i_1 - 1} = 4$ sequences

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

of $s^{(i_2)}$ correspond to a sequence {1010} of $s^{(i_1+1)}$.)

The above approach to constructing a 2^n-periodic binary sequence $s^{(n)}$ is based on the reverse process of Games-Chan algorithm (see Algorithm 2.1.1 in Section 2.1). The above relation is denoted as $u^{(n)} = GC^{-1}(u^{(i_j)}), 1 \leq j \leq m$, where GC represents the Games-Chan algorithm.

Now we consider the sum of two sequences $u^{(n)}$ and $v^{(n)}$. As both of them are constructed from $u^{(i)}$ and $v^{(i)}$ respectively, we now consider the sum of $u^{(i)}$ and $v^{(i)}$.

In the case of $u^{(i_1)} \neq v^{(i_1)}$, as both of them have only one nonzero element, so $L(u^{(i_1)} + v^{(i_1)}) = 2^{i_1} - 2^r$, where $r < i_1$. For example, in the case of $Left(u^{(i_1)} + v^{(i_1)}) = Right(u^{(i_1)} + v^{(i_1)})$, it is easy to see that $r = i_1 - 1$.

Next from the reverse process of Algorithm 2.1.1 in Section 2.1, we have $u^{(n)} + v^{(n)} = GC^{-1}(u^{(i_1)} + v^{(i_1)})$, thus $L(u^{(n)} + v^{(n)}) = 2^n - (2^{i_m} + 2^{i_{m-1}} + \cdots + 2^{i_1} + 2^r)$.

Now suppose that $u^{(i_1)} = v^{(i_1)}$, $u^{(i_2)} = v^{(i_2)}, \cdots, u^{(i_{j-1})} = v^{(i_{j-1})}$, but $u^{(r+1)} \neq v^{(r+1)}$ for $i_{j-1} < r < i_j$. In this case, we have

$$L(u^{(r+1)} + v^{(r+1)}) = 2^{r+1} - (2^r + \epsilon_{j-1} 2^{i_{j-1}} + \cdots + \epsilon_1 2^{i_1}),$$

where $i_{j-1} < r < i_j$. In consideration of the reverse process in Algorithm 2.1.1, we have

$$u^{(n)} + v^{(n)} = GC^{-1}(u^{(r+1)} + v^{(r+1)}) + s^{(n)},$$

where

$$L(s^{(n)}) \leq 2^n - (2^{i_m} + 2^{i_{m-1}} + \cdots + 2^{i_j} + 2^{r+1}) < L(GC^{-1}(u^{(r+1)} + v^{(r+1)}))$$

$$= 2^n - (2^{i_m} + 2^{i_{m-1}} + \cdots + 2^{i_j} + 2^r + \epsilon_{j-1}2^{i_{j-1}} + \cdots + \epsilon_1 2^{i_1}).$$

In this case, the linear complexity of $u^{(n)} + v^{(n)}$ will not be affected by $s^{(n)}$. Therefore,

$$L(u^{(n)} + v^{(n)}) = 2^n - (2^{i_m} + 2^{i_{m-1}} + \cdots + 2^{i_j} + 2^r + \epsilon_{j-1}2^{i_{j-1}} + \cdots + \epsilon_1 2^{i_1}),$$

where $\epsilon_1, \epsilon_2, \cdots, \epsilon_{j-1} \in \{0, 1\}$.

Recursively, suppose that $u^{(i_1)} = v^{(i_1)}$, $u^{(i_2)} = v^{(i_2)}, \cdots, u^{(i_m)} = v^{(i_m)}$, but $u^{(r+1)} \neq v^{(r+1)}$. In this case, we have

$$L(u^{(r+1)} + v^{(r+1)}) = 2^{r+1} - (2^r + \epsilon_m 2^{i_m} + \epsilon_{m-1}2^{i_{m-1}} + \cdots + \epsilon_1 2^{i_1}),$$

where $i_m < r < n$. Then from the reverse process of Algorithm 2.1.1, we have

$$u^{(n)} + v^{(n)} = GC^{-1}(u^{(r+1)} + v^{(r+1)}) + s^{(n)},$$

where

$$L(s^{(n)}) \leq 2^n - 2^{r+1} < L(GC^{-1}(u^{(r+1)} + v^{(r+1)})) = 2^n - (2^r + \epsilon_m 2^{i_m} + \epsilon_{m-1}2^{i_{m-1}} + \cdots + \epsilon_1 2^{i_1}).$$

Similarly we have,

$$L(u^{(n)} + v^{(n)}) = 2^n - (2^r + \epsilon_m 2^{i_m} + \epsilon_{m-1}2^{i_{m-1}} + \cdots + \epsilon_1 2^{i_1}),$$

where $\epsilon_1, \epsilon_2, \cdots, \epsilon_m \in \{0, 1\}$. This completes the proof. □

The following examples are given to illustrate the above formula.

Suppose that $n = 4, i_2 = 2, i_1 = 1$, $u^{(n)} = \{1010\ 1010\ 0000\ 0000\}, v^{(n)} = \{0000\ 0000\ 1010\ 1010\}$. Then $u^{(n)} + v^{(n)} = \{1010\ 1010\ 1010\ 1010\}$. Thus $L(u^{(n)} + v^{(n)}) = 2^4 - (2^3 + 2^2 + 2^1) = 2$, where $r = 3$.

Let $u^{(n)} = \{1010\ 1010\ 0000\ 0000\}, v^{(n)} = \{0101\ 0101\ 0000\ 0000\}$. Then $u^{(n)} + v^{(n)} = \{1111\ 1111\ 0000\ 0000\}$. Thus $L(u^{(n)} + v^{(n)}) = 2^4 - (2^2 + 2^1 + 2^0) = 9$, where $r = 0$.

Let $u^{(n)} = \{1010\ 0000\ 0000\ 1010\}, v^{(n)} = \{0000\ 0000\ 1010\ 1010\}$. Then $u^{(n)} + v^{(n)} = \{1010\ 0000\ 1010\ 0000\}$. Thus $L(u^{(n)} + v^{(n)}) = 2^4 - (2^3 + 2^1) = 6$, where $r = 3, \epsilon_2 = 0$.

Let $u^{(n)} = \{1000\ 1000\ 0010\ 0010\}, v^{(n)} = \{0000\ 0000\ 1010\ 1010\}$. Then $u^{(n)} + v^{(n)} = \{1000\ 1000\ 1000\ 1000\}$. Thus $L(u^{(n)} + v^{(n)}) = 2^4 - (2^3 + 2^2) = 4$, where $r = 3, \epsilon_1 = 0$.

Here $L(u^{(n)}) = L(v^{(n)}) = 2^4 - (2^2 + 2^1), W_H(u^{(n)}) = W_H(v^{(n)}) = 2^2$.

Suppose that $n = 4, i_2 = 1, i_1 = 0, r = 2$, $u^{(n)} = \{1111\ 0000\ 0000\ 0000\}, v^{(n)} = \{0110\ 1000\ 0001\ 0000\}$. Then $u^{(r+1)} + v^{(r+1)} = \{1000\ 1000\}$, $GC^{-1}(u^{(r+1)} + v^{(r+1)}) = \{1000\ 10000000\ 0000\}$,

$s^{(n)} = \{0001\ 0000\ 0001\ 0000\}, u^{(n)} + v^{(n)} = \{1001\ 1000\ 0001\ 0000\} = GC^{-1}(u^{(r+1)} + v^{(r+1)}) + s^{(n)}$.

As $L(s^{(n)}) = 2^4 - 2^3 < L(GC^{-1}(u^{(r+1)} + v^{(r+1)})) = 2^4 - 2^2$, thus $L(u^{(n)} + v^{(n)}) = 2^4 - 2^2 = 12$, where $\epsilon_2 = 0$, $\epsilon_1 = 0$.

Before we turn to the main problem, we briefly discuss representation of the minimum Hamming weight for a sequence. Suppose that $s^{(n)}$ is a 2^n-periodic binary sequence with linear complexity $2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m})$ and the minimum Hamming weight. From Theorem 2.7.1, $W_H(s^{(n)}) \leq 2^m$. Next, it is impossible that $W_H(s^{(n)}) < 2^m$. If $W_H(s^{(n)}) < 2^m$, then the minimum number k for which the k-error linear complexity of $s^{(n)}$ is strictly less than the linear complexity of $s^{(n)}$ is $W_H(s^{(n)})$. This contradicts the result by Kurosawa *et al.* (2000) that the minimum number k for which the k-error linear complexity of 2^n-periodic binary sequence $s^{(n)}$ is strictly less than the linear complexity of $s^{(n)}$ is 2^m. Thus the Hamming weight of $s^{(n)}$ must be 2^m.

Let $s^{(n)}$ be a 2^n-periodic binary sequence with linear complexity $2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m})$. To consider $L_{2^m}(s^{(n)})$, we just need to compute $L(s^{(n)} + u^{(n)})$, where $u^{(n)}$ is a 2^n-periodic binary sequence with linear complexity $2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m})$ and $W_H(u^{(n)}) = 2^m$.

Now we investigate the first descent point (critical point) distribution of the k-error linear complexity, namely, the possible values of the 2^m-error linear complexity. By Kurosawa *et al.* (2000), we know that the first descent point of the k-error linear complexity is $k = 2^m$, where $0 \leq m \leq n$. So our concern turns to the distribution of 2^m-error linear complexity, which is given in the following theorem.

Theorem 2.7.3 Let $s^{(n)}$ be a 2^n-periodic binary sequence with linear complexity $2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m})$, where $0 \leq i_1 < i_2 < \cdots < i_m < n$. Then

$$L_{2^m}(s^{(n)}) = \begin{cases} 2^n - (2^{i_m} + 2^{i_{m-1}} + \cdots + 2^{i_1}) - 2^{r+1} + c, \\ \qquad 1 \le r \le i_1 - 1, 1 \le c \le 2^r - 1 \\ 2^n - (2^{i_m} + 2^{i_{m-1}} + \cdots + 2^{i_2}) - 2^{r+1} + c, \\ \qquad i_1 + 1 \le r \le i_2 - 1, 1 \le c \le 2^r - 1, c \ne 2^r - 2^{i_1} \\ 2^n - (2^{i_m} + 2^{i_{m-1}} + \cdots + 2^{i_3}) - 2^{r+1} + c, \\ \qquad i_2 + 1 \le r \le i_3 - 1, 1 \le c \le 2^r - 1, c \ne 2^r - \epsilon_1 2^{i_1} - \epsilon_2 2^{i_2} \\ \cdots\cdots \\ 2^n - 2^{r+1} + c, \\ \qquad i_m + 1 \le r \le n - 1, 1 \le c \le 2^r - 1, c \ne 2^r - \epsilon_1 2^{i_1} - \epsilon_2 2^{i_2} - \cdots - \epsilon_m 2^{i_m} \end{cases},$$

where $\epsilon_1, \epsilon_2, \cdots, \epsilon_m \in \{0, 1\}$.

Proof. The following proof is based on the property for the sum of two sequences in the framework: $S + E = \{t + e | t \in S, e \in E\}$, where t is a sequence with linear complexity c and e is sequence with $W_H(e) = 2^m$ and linear complexity $L(e) = 2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m})$, $0 \le i_1 < i_2 < \cdots < i_m < n$, and $L(t + e) = L(e)$. With the sieve method, we aim to sieve sequences $t + e$ with $L_{2^m}(t + e) = c$ from $S + E$.

For a given linear complexity c, it remains to investigate the case that $t + u \in S + E$, but $L_{2^m}(t + u) < c$. As observed from the following proof that this is equivalent to checking if there exists a sequence v such that $L(u + v) = c$. We try to exclude this case in the sieving process.

As $s^{(n)}$ is a 2^n-periodic binary sequence with linear complexity $2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m})$, by Kurosawa *et al.* (2000), $L_{2^m}(s^{(n)}) < 2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m})$.

First we prove that $L_{2^m}(s^{(n)}) \ne 2^n - (\epsilon_m 2^{i_m} + \epsilon_{m-1} 2^{i_{m-1}} + \cdots + \epsilon_1 2^{i_1} + 2^r)$, where $r \in \{n - 1, n - 2, \cdots\cdots, 1, 0\} \setminus \{i_1, i_2, \cdots, i_m\}$ and $\epsilon_1, \epsilon_2, \cdots, \epsilon_m \in \{0, 1\}$.

We prove it by a contradiction checking. Suppose that $L_{2^m}(s^{(n)}) = 2^n - (\epsilon_m 2^{i_m} + \epsilon_{m-1} 2^{i_{m-1}} + \cdots + \epsilon_1 2^{i_1} + 2^r) < 2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m})$. Then $s^{(n)} = t^{(n)} + u^{(n)}$, where $t^{(n)}$ is a 2^n-periodic binary sequence with linear complexity $2^n - (\epsilon_m 2^{i_m} + \epsilon_{m-1} 2^{i_{m-1}} + \cdots + \epsilon_1 2^{i_1} + 2^r)$, and $u^{(n)}$ is a 2^n-periodic binary sequence with linear complexity $2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m})$ and $W_H(u^{(n)}) = 2^m$. From Remark 2.1.1 in Section 2.1 and Theorem 2.7.2, there exists a 2^n-periodic binary sequence $v^{(n)}$ with linear complexity $2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m})$ and $W_H(v^{(n)}) = 2^m$, such that $L(u^{(n)} + v^{(n)}) = 2^n - (\epsilon_m 2^{i_m} + \epsilon_{m-1} 2^{i_{m-1}} + \cdots + \epsilon_1 2^{i_1} + 2^r)$. From Lemma 2.1.2 in Section 2.1, $L(t^{(n)} + u^{(n)} + v^{(n)}) < 2^n - (\epsilon_m 2^{i_m} + \epsilon_{m-1} 2^{i_{m-1}} + \cdots + \epsilon_1 2^{i_1} + 2^r)$,

thus $L_{2^m}(t^{(n)}+u^{(n)}) < 2^n-(\epsilon_m 2^{i_m}+\epsilon_{m-1}2^{i_{m-1}}+\cdots+\epsilon_1 2^{i_1}+2^r)$. This is a contradiction, which completes the proof of this assertion.

Next consider the case that $L_{2^m}(s^{(n)}) = 2^n-(2^{i_m}+2^{i_{m-1}}+\cdots+2^{i_1})-2^{r+1}+c$, where $1 \le c \le 2^r-1$. In this case, let $t^{(n)}$ be a 2^n-periodic binary sequence with linear complexity $2^n-(2^{i_m}+2^{i_{m-1}}+\cdots+2^{i_1})-2^{r+1}+c, 1 \le r \le i_1-1, 1 \le c \le 2^r-1$. Let $u^{(n)}$ be a 2^n-periodic binary sequence with linear complexity $2^n-(2^{i_1}+2^{i_2}+\cdots+2^{i_m})$ and $W_H(u^{(n)}) = 2^m$. Then from Lemma 2.1.2 in Section 2.1, $L(t^{(n)}+u^{(n)}) = 2^n-(2^{i_m}+2^{i_{m-1}}+\cdots+2^{i_1})$. Now it remains to prove that $L_{2^m}(t^{(n)}+u^{(n)}) = 2^n-(2^{i_m}+2^{i_{m-1}}+\cdots+2^{i_1})-2^{r+1}+c$.

Suppose that $v^{(n)}$ is a 2^n-periodic binary sequence with linear complexity $2^n-(2^{i_1}+2^{i_2}+\cdots+2^{i_m})$ and $W_H(v^{(n)}) = 2^m$, $u^{(n)} \ne v^{(n)}$. One can derive from Theorem 2.7.2 that, $L(u^{(n)}+v^{(n)}) = 2^n-(\epsilon_m 2^{i_m}+\epsilon_{m-1}2^{i_{m-1}}+\cdots+\epsilon_1 2^{i_1}+2^r) \ne 2^n-(2^{i_m}+2^{i_{m-1}}+\cdots+2^{i_1}+2^{r+1})+c$.

If $L(u^{(n)}+v^{(n)}) < 2^n-(2^{i_m}+2^{i_{m-1}}+\cdots+2^{i_1}+2^{r+1})+c$, then from Lemma 2.1.2 $L(t^{(n)}+u^{(n)}+v^{(n)}) = 2^n-(2^{i_m}+2^{i_{m-1}}+\cdots+2^{i_1})-2^{r+1}+c$.

If $L(u^{(n)}+v^{(n)}) > 2^n-(2^{i_m}+2^{i_{m-1}}+\cdots+2^{i_1}+2^{r+1})+c$, similarly we have $L(t^{(n)}+u^{(n)}+v^{(n)}) > 2^n-(2^{i_m}+2^{i_{m-1}}+\cdots+2^{i_1})-2^{r+1}+c$.

Note that $L(t^{(n)}+u^{(n)}+u^{(n)}) = L(t^{(n)}) = 2^n-(2^{i_m}+2^{i_{m-1}}+\cdots+2^{i_1})-2^{r+1}+c$. In summary of these three situations, we can conclude that $L_{2^m}(t^{(n)}+u^{(n)}) = 2^n-(2^{i_m}+2^{i_{m-1}}+\cdots+2^{i_1})-2^{r+1}+c$.

Similarly, theorem can be proved to be true on other cases for parameters r and c. □

Secondly, based on the first descent point distribution, we can derive the complete counting functions on the number of 2^n-periodic binary sequences with given 2^m-error linear complexity corresponding to different cases in Theorem 2.7.3.

Theorem 2.7.4 Let $N_{2^m}(L)$ be the number of 2^n-periodic binary sequences $s^{(n)}$ with linear complexity $2^n-(2^{i_1}+2^{i_2}+\cdots+2^{i_m})$ and the 2^m-error linear complexity L taking different values, for any fixed $0 \le i_1 < i_2 < \cdots < i_m < n$. Then

$$N_{2^m}(L) = \begin{cases} 2^{2^m n - 2^{m-1} i_m - \cdots - 2i_2 - i_1 - 2^{m+1} + 2}, & L = 0 \\ 2^{L+r}, & L = 2^n - (2^{i_m} + 2^{i_{m-1}} + \cdots + 2^{i_1}) - 2^{r+1} + c, \\ & 1 \le r \le i_1 - 1, 1 \le c < 2^r \\ 2^{L+2r-i_1-1}, & L = 2^n - (2^{i_m} + 2^{i_{m-1}} + \cdots + 2^{i_2}) - 2^{r+1} + c, \\ & i_1 + 1 \le r \le i_2 - 1, 1 \le c < 2^r - 2^{i_1} \\ 2^{L+2r-i_1-2}, & L = 2^n - (2^{i_m} + 2^{i_{m-1}} + \cdots + 2^{i_2}) - 2^{r+1} + c, \\ & i_1 + 1 \le r \le i_2 - 1, 2^r - 2^{i_1} < c < 2^r \\ 2^{L+4r-2i_2-i_1-3}, & L = 2^n - (2^{i_m} + 2^{i_{m-1}} + \cdots + 2^{i_3}) - 2^{r+1} + c, \\ & i_2 + 1 \le r \le i_3 - 1, 1 \le c < 2^r - 2^{i_1} - 2^{i_2} \\ 2^{L+4r-2i_2-i_1-4}, & L = 2^n - (2^{i_m} + 2^{i_{m-1}} + \cdots + 2^{i_3}) - 2^{r+1} + c, \\ & i_2 + 1 \le r \le i_3 - 1, 2^r - 2^{i_1} - 2^{i_2} < c < 2^r - 2^{i_2} \\ 2^{L+4r-2i_2-i_1-5}, & L = 2^n - (2^{i_m} + 2^{i_{m-1}} + \cdots + 2^{i_3}) - 2^{r+1} + c, \\ & i_2 + 1 \le r \le i_3 - 1, 2^r - 2^{i_2} < c < 2^r - 2^{i_1} \\ 2^{L+4r-2i_2-i_1-6}, & L = 2^n - (2^{i_m} + 2^{i_{m-1}} + \cdots + 2^{i_3}) - 2^{r+1} + c, \\ & i_2 + 1 \le r \le i_3 - 1, 2^r - 2^{i_1} < c < 2^r \\ \cdots\cdots & \\ 2^{L+2^m r - 2^{m-1} i_m - \cdots - 2i_2 - i_1 - 2^{m+1} + 1}, & L = 2^n - 2^{r+1} + c, \\ & i_m + 1 \le r \le n - 1, 2^r - 2^{i_2} < c < 2^r - 2^{i_1} \\ 2^{L+2^m r - 2^{m-1} i_m - \cdots - 2i_2 - i_1 - 2^{m+1} + 2}, & L = 2^n - 2^{r+1} + c, \\ & i_m + 1 \le r \le n - 1, 2^r - 2^{i_1} < c < 2^r \\ 0, & \text{otherwise} \end{cases}$$

Proof. By Theorem 2.7.1, we know that $N_{2^m}(0) = 2^{2^m n - 2^{m-1} i_m - \cdots - 2i_2 - i_1 - 2^{m+1} + 2}$.

Similar to the proof of Theorem 2.7.3, the following proof is based on the property on the sum of two sequences in the framework: $S + E = \{t + e | t \in S, e \in E\}$, where t is a sequence with linear complexity c and e is sequence with $W_H(e) = 2^m$ and linear complexity $L(e) = 2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m})$, $0 \le i_1 < i_2 < \cdots < i_m < n$, and $L(t+e) = L(e)$. With the sieve method, we aim to sieve sequences $t+e$ with $L_{2^m}(t+e) = c$ from $S + E$.

For a given linear complexity c, it remains to investigate the case that $s+u, t+v \in S+E$ and $L_{2^m}(s+u) = L_{2^m}(t+v) = c$ with $s \neq t$, $u \neq v$, but $s+u = t+v$. This is equivalent to checking if there exists a sequence v such that $L(u+v) = L(s+t) < c$ and if so, calculating the number of such sequences v, where $W_H(u) = W_H(v) = 2^m$.

Based on Algorithm 2.1.1, in the kth step, $1 \le k \le n$, if and only if one period of the

sequence can not be divided into two equal parts, then the linear complexity should be increased by half period. In the kth step, the linear complexity can be increased by maximum 2^{n-k}.

1) Now we consider the case $L = 2^n - (2^{i_m} + 2^{i_{m-1}} + \cdots + 2^{i_1}) - 2^{r+1} + c, 1 \le r \le i_1 - 1, 1 \le c \le 2^r - 1$. Let $s^{(n)}$ be a 2^n-periodic binary sequence with linear complexity L. Based on Algorithm 2.1.1, after the $n-(r+1)$th step, the period of the sequence $s^{(r+1)}$ becomes 2^{r+1}, the linear complexity of the sequence $s^{(r+1)}$ is c. By Lemma 2.1.6 in Section 2.1, the number of binary sequences with linear complexity c is 2^{c-1}.

By changing any one element, a given sequence $s^{(r+1)}$ can be changed to a sequence $t^{(r+1)}$ with linear complexity 2^{r+1}. Thus the number of such new binary sequences $t^{(r+1)}$ with linear complexity 2^{r+1} is $2^{r+1} \times 2^{c-1}$.

For a given sequence $t^{(r+1)}$ with linear complexity 2^{r+1}, restore the sequence $t^{(n)}$ with linear complexity $2^n - (2^{i_m} + 2^{i_{m-1}} + \cdots + 2^{i_1})$ from $t^{(r+1)}$ by the reverse process of Algorithm 2.1.1. By Lemma 2.1.5 in Section 2.1, $2^{2^n-(2^{i_m}+2^{i_{m-1}}+\cdots+2^{i_1})-2^{r+1}}$ sequences $t^{(n)}$ will be obtained.

Specifically, when we restore the sequence $t^{(n)}$ with linear complexity 2^n from $t^{(r+1)}$ by the reverse process of Algorithm 2.1.1, by Lemma 2.1.5 in Section 2.1, the number of sequences $t^{(n)}$ will be $2^{2^{r+1}+2^{r+2}+\cdots+2^{n-1}} = 2^{2^n-2^{r+1}}$. For the sequence $t^{(n)}$ with linear complexity $2^n - (2^{i_m} + 2^{i_{m-1}} + \cdots + 2^{i_1})$, from Algorithm 2.1.1, there are m steps that one period of the sequence can be divided into two equal parts, thus the number of sequences $t^{(n)}$ will be $2^{2^n-2^{r+1}-(2^{i_m}+2^{i_{m-1}}+\cdots+2^{i_1})}$.

The total number of such sequence $t^{(n)}$ is

$$2^{2^n-(2^{i_m}+2^{i_{m-1}}+\cdots+2^{i_1})-2^{r+1}} \times 2^{r+1} \times 2^{c-1} = 2^{2^n-(2^{i_m}+2^{i_{m-1}}+\cdots+2^{i_1})-2^{r+1}+c+r}.$$

Note that by changing any one element, a given sequence $s^{(r+1)}$ with the linear complexity c can be changed to a sequence $t^{(r+1)}$ with linear complexity 2^{r+1}. Thus new sequence $t^{(n)} = u^{(n)} + s^{(n)}$, where $s^{(n)}$ is a 2^n-periodic binary sequence with linear complexity $2^n - (2^{i_m} + 2^{i_{m-1}} + \cdots + 2^{i_1}) - 2^{r+1} + c$, $u^{(n)}$ is a 2^n-periodic binary sequence with linear complexity $2^n - (2^{i_m} + 2^{i_{m-1}} + \cdots + 2^{i_1})$ and $W_H(u^{(n)}) = 2^m$. From Theorem 2.7.3, $L_{2^m}(t^{(n)}) = 2^n - (2^{i_m} + 2^{i_{m-1}} + \cdots + 2^{i_1}) - 2^{r+1} + c$.

2) Consider the case $L = 2^n - (2^{i_m} + 2^{i_{m-1}} + \cdots + 2^{i_2}) - 2^{r+1} + c, i_1 + 1 \le r \le i_2 - 1, 1 \le c < 2^r - 2^{i_1}$. Let $t^{(n)}$ be a 2^n-periodic binary sequence with linear complexity L. Based

on Algorithm 2.1.1, after the $n-(r+1)$th step, the period of the sequence $t^{(r+1)}$ becomes 2^{r+1}, the linear complexity of the sequence $t^{(r+1)}$ is c. By Lemma 2.1.6 in Section 2.1, the number of binary sequences with linear complexity c is 2^{c-1}.

Let $u^{(r+1)}$ be a 2^{r+1}-periodic sequence with linear complexity $2^{r+1}-2^{i_1}$ and $W_H(u^{(r+1)}) = 2$. By Theorem 2.7.1, the number of sequences $u^{(r+1)}$ with linear complexity $2^{r+1}-2^{i_1}$ is $2^{2(r+1)-i_1-2} = 2^{2r-i_1}$. Thus the number of sequences $t^{(r+1)}+u^{(r+1)}$ with linear complexity $2^{r+1}-2^{i_1}$ is $2^{2r-i_1} \times 2^{c-1}$.

For a given sequence $t^{(r+1)}+u^{(r+1)}$ with linear complexity $2^{r+1}-2^{i_1}$, we restore the sequence $t^{(r+1)}+u^{(r+1)}$ to $t^{(n)}+u^{(n)}$ with linear complexity $2^n-(2^{i_m}+2^{i_{m-1}}+\cdots+2^{i_1})$ by the reverse process of Algorithm 2.1.1. By Lemma 2.1.5 in Section 2.1, $2^{2^n-(2^{i_m}+2^{i_{m-1}}+\cdots+2^{i_2})-2^{r+1}}$ sequences $t^{(n)}+u^{(n)}$ will be obtained. The number of such sequences $t^{(n)}+u^{(n)}$ is

$$2^{2^n-(2^{i_m}+2^{i_{m-1}}+\cdots+2^{i_2})-2^{r+1}} \times 2^{2r-i_1} \times 2^{c-1} = 2^{2^n-(2^{i_m}+2^{i_{m-1}}+\cdots+2^{i_2})-2^{r+1}+c-1+2r-i_1},$$

where $u^{(n)}$ is a 2^n-periodic binary sequence with linear complexity $2^n-(2^{i_m}+2^{i_{m-1}}+\cdots+2^{i_1})$ and $W_H(u^{(n)}) = 2^m$. Also from Theorem 2.7.3, $L_{2^m}(t^{(n)}+u^{(n)}) = 2^n-(2^{i_m}+2^{i_{m-1}}+\cdots+2^{i_2})-2^{r+1}+c$.

3) Consider the case of $L = 2^n-(2^{i_m}+2^{i_{m-1}}+\cdots+2^{i_2})-2^{r+1}+c, i_1+1 \le r \le i_2-1, 2^r-2^{i_1} < c < 2^r-1$. Let $t^{(n)}$ be a 2^n-periodic binary sequence with linear complexity L. Based on Algorithm 2.1.1, after the $n-(r+1)$th step, the period of the sequence $t^{(r+1)}$ becomes 2^{r+1}, the linear complexity of the sequence $t^{(r+1)}$ is c. By Lemma 2.1.6 in Section 2.1, the number of binary sequences with linear complexity c is 2^{c-1}.

Let $u^{(r+1)}$ be a 2^{r+1}-periodic sequence with linear complexity $2^{r+1}-2^{i_1}$ and $W_H(u^{(r+1)}) = 2$. By Theorem 2.7.1, the number of sequences $t^{(r+1)}+u^{(r+1)}$ with linear complexity $2^{r+1}-2^{i_1}$ is $2^{2r-i_1} \times 2^{c-1}$.

Let $S = \{s|L(s) = c\}, E = \{e|W_H(e) = 2\}, S+E = \{s+e|s \in S, e \in E\}$, where s is a sequence with linear complexity c and e is sequence with $W_H(e) = 2$ and linear complexity $L(e) = 2^{r+1}-2^{i_1}$. With the sieve method, we aim to sieve sequences $s+e$ with $L_2(s+e) = c$ from $S+E$.

It remains to investigate the case that $s, t \in S, u, v \in E$ and $L_2(s+u) = L_2(t+v) = c$ with $s \neq t$, $u \neq v$, but $s+u = t+v$. It is equivalent to checking if there exists a sequence v such that $L(u+v) = L(s+t) < c$ and if so, check the number of such sequence v, where $W_H(u) = W_H(v) = 2$.

For any sequence $u^{(r+1)}$, by Theorem 2.7.2, there exists exactly one sequence $v^{(r+1)}$ with linear complexity $2^{r+1}-2^{i_1}$ and $W_H(u^{(r+1)})=2$, such that $L(u^{(r+1)}+v^{(r+1)})=2^r-2^{i_1}<c$.

(The following example is given to illustrate the above case. Suppose that $r=3, i_1=1$, $u^{(4)}=\{1010\ 0000\ 0000\ 0000\}, v^{(4)}=\{0000\ 0000\ 1010\ 0000\}$. Then $u^{(4)}+v^{(4)}=\{1010\ 0000\ 1010\ 0000\}$. Thus $L(u^{(4)}+v^{(4)})=2^4-(2^3+2^1)=2^3-2^1$.)

Let $x^{(r+1)}=t^{(r+1)}+u^{(r+1)}+v^{(r+1)}$. Then $L(x^{(r+1)})=c$, $t^{(r+1)}+u^{(r+1)}=x^{(r+1)}+v^{(r+1)}$. Therefore, the number of distinct sequences $t^{(r+1)}+u^{(r+1)}$ with linear complexity $2^{r+1}-2^{i_1}$ is $2^{2r-i_1-1}\times 2^{c-1}$.

For a given sequence $t^{(r+1)}+u^{(r+1)}$ with linear complexity $2^{r+1}-2^{i_1}$, we restore sequence $t^{(r+1)}+u^{(r+1)}$ to $t^{(n)}+u^{(n)}$ with linear complexity $2^n-(2^{i_m}+2^{i_{m-1}}+\cdots+2^{i_1})$ by the reverse process of Algorithm 2.1.1. By Lemma 2.1.5 in Section 2.1, $2^{2^n-(2^{i_m}+2^{i_{m-1}}+\cdots+2^{i_2})-2^{r+1}}$ sequences $t^{(n)}+u^{(n)}$ will be obtained. The number of such sequences $t^{(n)}+u^{(n)}$ is

$$2^{2^n-(2^{i_m}+2^{i_{m-1}}+\cdots+2^{i_2})-2^{r+1}}\times 2^{2r-i_1-1}\times 2^{c-1}=2^{2^n-(2^{i_m}+2^{i_{m-1}}+\cdots+2^{i_2})-2^{r+1}+c-2+2r-i_1},$$

where $u^{(n)}$ is a 2^n-periodic binary sequence with linear complexity $2^n-(2^{i_m}+2^{i_{m-1}}+\cdots+2^{i_1})$ and $W_H(u^{(n)})=2^m$. Also from Theorem 2.7.3, $L_{2^m}(t^{(n)}+u^{(n)})=2^n-(2^{i_m}+2^{i_{m-1}}+\cdots+2^{i_2})-2^{r+1}+c$.

4) When $L=2^n-(2^{i_m}+2^{i_{m-1}}+\cdots+2^{i_3})-2^{r+1}+c, i_2+1\le r\le i_3-1, 1\le c<2^r-(2^{i_2}+2^{i_1})$, let $t^{(n)}$ be a 2^n-periodic binary sequence with linear complexity L. Based on Algorithm 2.1.1, after the $n-(r+1)$th step, the period of the sequence $t^{(r+1)}$ becomes 2^{r+1}, the linear complexity of the sequence $t^{(r+1)}$ is c.

Let $u^{(r+1)}$ be a 2^{r+1}-periodic sequence with linear complexity $2^{r+1}-(2^{i_2}+2^{i_1})$ and $W_H(u^{(r+1)})=2^2$. By Theorem 2.7.1, the number of sequences $t^{(r+1)}+u^{(r+1)}$ with linear complexity $2^{r+1}-(2^{i_2}+2^{i_1})$ is $2^{4r-2i_2-i_1-2}\times 2^{c-1}$.

For a given sequence $t^{(r+1)}+u^{(r+1)}$ with linear complexity $2^{r+1}-(2^{i_2}+2^{i_1})$, restore sequence $t^{(r+1)}+u^{(r+1)}$ to $t^{(n)}+u^{(n)}$ with linear complexity $2^n-(2^{i_m}+2^{i_{m-1}}+\cdots+2^{i_1})$ by the reverse process of Algorithm 2.1.1. By Lemma 2.1.5 in Section 2.1, $2^{2^n-(2^{i_m}+2^{i_{m-1}}+\cdots+2^{i_3})-2^{r+1}}$ sequence $t^{(n)}+u^{(n)}$ will be obtained. The number of such sequences $t^{(n)}+u^{(n)}$ is

$$2^{2^n-(2^{i_m}+2^{i_{m-1}}+\cdots+2^{i_2})-2^{r+1}}\times 2^{4r-2i_2-i_1-2}\times 2^{c-1}=2^{2^n-(2^{i_m}+2^{i_{m-1}}+\cdots+2^{i_2})-2^{r+1}+c+4r-2i_2-i_1-3},$$

where $u^{(n)}$ is a 2^n-periodic binary sequence with linear complexity $2^n-(2^{i_m}+2^{i_{m-1}}+\cdots+2^{i_1})$ and $W_H(u^{(n)})=2^m$. Also $L_{2^m}(t^{(n)}+u^{(n)})=2^n-(2^{i_m}+2^{i_{m-1}}+\cdots+2^{i_3})-2^{r+1}+c$.

5) If $L = 2^n - (2^{i_m} + 2^{i_{m-1}} + \cdots + 2^{i_3}) - 2^{r+1} + c, i_2 + 1 \le r \le i_3 - 1, 2^r - (2^{i_2} + 2^{i_1}) < c < 2^r - 2^{i_2}$, let $t^{(n)}$ be a 2^n-periodic binary sequence with linear complexity L. Based on Algorithm 2.1.1, after the $n - (r+1)$th step, the period of the sequence $t^{(r+1)}$ becomes 2^{r+1}, the linear complexity of the sequence $t^{(r+1)}$ is c.

Let $u^{(r+1)}$ be a 2^{r+1}-periodic sequence with linear complexity $2^{r+1} - (2^{i_2} + 2^{i_1})$ and $W_H(u^{(r+1)}) = 2^2$. By Theorem 2.7.1, the number of sequences $t^{(r+1)} + u^{(r+1)}$ with linear complexity $2^{r+1} - (2^{i_2} + 2^{i_1})$ is $2^{4r-2i_2-i_1-2} \times 2^{c-1}$.

For any sequence $u^{(r+1)}$, by Theorem 2.7.2, there exists exactly one sequence $v^{(r+1)}$ with linear complexity $2^{r+1} - (2^{i_2} + 2^{i_1})$ and $W_H(u^{(r+1)}) = 2^2$, such that $L(u^{(r+1)} + v^{(r+1)}) = 2^r - (2^{i_2} + 2^{i_1}) < c$. Let $x^{(r+1)} = t^{(r+1)} + u^{(r+1)} + v^{(r+1)}$. Then $L(x^{(r+1)}) = c$, $t^{(r+1)} + u^{(r+1)} = x^{(r+1)} + v^{(r+1)}$. Therefore, the number of distinct sequences $t^{(r+1)} + u^{(r+1)}$ with linear complexity $2^{r+1} - (2^{i_2} + 2^{i_1})$ is $2^{4r-2i_2-i_1-3} \times 2^{c-1}$.

For a given sequence $t^{(r+1)} + u^{(r+1)}$ with linear complexity $2^{r+1} - (2^{i_2} + 2^{i_1})$, restore the sequence $t^{(r+1)} + u^{(r+1)}$ to $t^{(n)} + u^{(n)}$ with linear complexity $2^n - (2^{i_m} + 2^{i_{m-1}} + \cdots + 2^{i_1})$ by the reverse process of Algorithm 2.1.1. By Lemma 2.1.5 in Section 2.1, $2^{2^n - (2^{i_m} + 2^{i_{m-1}} + \cdots + 2^{i_3}) - 2^{r+1}}$ sequences $t^{(n)} + u^{(n)}$ will be obtained. The number of such sequences $t^{(n)} + u^{(n)}$ is

$$2^{2^n - (2^{i_m} + 2^{i_{m-1}} + \cdots + 2^{i_3}) - 2^{r+1}} \times 2^{4r-2i_2-i_1-3} \times 2^{c-1} = 2^{2^n - (2^{i_m} + 2^{i_{m-1}} + \cdots + 2^{i_3}) - 2^{r+1} + c + 4r - 2i_2 - i_1 - 4},$$

where $u^{(n)}$ is a 2^n-periodic binary sequence with linear complexity $2^n - (2^{i_m} + 2^{i_{m-1}} + \cdots + 2^{i_1})$ and $W_H(u^{(n)}) = 2^m$. Also from Theorem 2.7.3, $L_{2^m}(t^{(n)} + u^{(n)}) = 2^n - (2^{i_m} + 2^{i_{m-1}} + \cdots + 2^{i_3}) - 2^{r+1} + c$.

6) If $L = 2^n - (2^{i_m} + 2^{i_{m-1}} + \cdots + 2^{i_3}) - 2^{r+1} + c, i_2 + 1 \le r \le i_3 - 1, 2^r - 2^{i_2} < c < 2^r - 2^{i_1}$, let $t^{(n)}$ be a 2^n-periodic binary sequence with linear complexity L. Based on Algorithm 2.1.1, after the $n - (r+1)$th step, the period of the sequence $t^{(r+1)}$ becomes 2^{r+1}, the linear complexity of the sequence $t^{(r+1)}$ is c.

Let $u^{(r+1)}$ be a 2^{r+1}-periodic sequence with linear complexity $2^{r+1} - (2^{i_2} + 2^{i_1})$ and $W_H(u^{(r+1)}) = 2^2$. By Theorem 2.7.1, the number of sequences $t^{(r+1)} + u^{(r+1)}$ with linear complexity $2^{r+1} - (2^{i_2} + 2^{i_1})$ is $2^{4r-2i_2-i_1-2} \times 2^{c-1}$.

For any sequence $u^{(r+1)}$, by Theorem 2.7.2, there exists exactly one sequence $v^{(r+1)}$ with linear complexity $2^{r+1} - (2^{i_2} + 2^{i_1})$ and $W_H(u^{(r+1)}) = 2^2$, such that $L(u^{(r+1)} + v^{(r+1)}) = 2^r - (2^{i_2} + 2^{i_1}) < c$.

There exist two sequences $v^{(r+1)}$ with linear complexity $2^{r+1}-(2^{i_2}+2^{i_1})$ and $W_H(u^{(r+1)}) = 2^2$, such that $L(u^{(r+1)} + v^{(r+1)}) = 2^r - 2^{i_2} < c$.

(The following example is given to illustrate the above case. Suppose that $r+1 = 4, i_2 = 2, i_1 = 1$, $u^{(r+1)} = \{1010\ 1010\ 0000\ 0000\}, v^{(r+1)} = \{0000\ 0000\ 1010\ 1010\}$. Then $u^{(r+1)} + v^{(r+1)} = \{1010\ 1010\ 1010\ 1010\}$. Thus $L(u^{(r+1)} + v^{(r+1)}) = 2^4 - (2^3 + 2^2 + 2^1) = 2$.

Let $v^{(r+1)} = \{0010\ 0010\ 1000\ 1000\}$. Then $u^{(r+1)} + v^{(r+1)} = \{1000\ 1000\ 1000\ 1000\}$. Thus $L(u^{(r+1)} + v^{(r+1)}) = 2^4 - (2^3 + 2^2) = 4$.

Let $v^{(r+1)} = \{1000\ 1000\ 0010\ 0010\}$. Then $u^{(r+1)} + v^{(r+1)} = \{0010\ 0010\ 0010\ 0010\}$. Thus $L(u^{(r+1)} + v^{(r+1)}) = 2^4 - (2^3 + 2^2) = 4$.

Here $L(u^{(r+1)}) = L(v^{(r+1)}) = 2^4 - (2^2 + 2^1), W_H(u^{(r+1)}) = W_H(v^{(r+1)}) = 2^2$.)

Let $x^{(r+1)} = t^{(r+1)} + u^{(r+1)} + v^{(r+1)}$. Then $L(x^{(r+1)}) = c$, $t^{(r+1)} + u^{(r+1)} = x^{(r+1)} + v^{(r+1)}$. Therefore, the number of distinct sequences $t^{(r+1)} + u^{(r+1)}$ with linear complexity $2^{r+1} - (2^{i_2} + 2^{i_1})$ is

$$2^{4r-2i_2-i_1-2} \times \frac{1}{2^2} \times 2^{c-1}.$$

For a given sequence $t^{(r+1)} + u^{(r+1)}$ with linear complexity $2^{r+1} - (2^{i_2} + 2^{i_1})$, restore the sequence $t^{(r+1)} + u^{(r+1)}$ to $t^{(n)} + u^{(n)}$ with linear complexity $2^n - (2^{i_m} + 2^{i_{m-1}} + \cdots + 2^{i_1})$ by the reverse process of Algorithm 2.1.1. By Lemma 2.1.5 in Section 2.1, $2^{2^n-(2^{i_m}+2^{i_m-1}+\cdots+2^{i_3})-2^{r+1}}$ sequences $t^{(n)} + u^{(n)}$ will be obtained. The number of such sequences $t^{(n)} + u^{(n)}$ is

$$2^{2^n-(2^{i_m}+2^{i_m-1}+\cdots+2^{i_3})-2^{r+1}} \times 2^{4r-2i_2-i_1-4} \times 2^{c-1} = 2^{2^n-(2^{i_m}+2^{i_m-1}+\cdots+2^{i_3})-2^{r+1}+c+4r-2i_2-i_1-5},$$

where $u^{(n)}$ is a 2^n-periodic binary sequence with linear complexity $2^n - (2^{i_m} + 2^{i_{m-1}} + \cdots + 2^{i_1})$ and $W_H(u^{(n)}) = 2^m$. Also $L_{2^m}(t^{(n)} + u^{(n)}) = 2^n - (2^{i_m} + 2^{i_{m-1}} + \cdots + 2^{i_3}) - 2^{r+1} + c$.

7) If $L = 2^n - (2^{i_m} + 2^{i_{m-1}} + \cdots + 2^{i_3}) - 2^{r+1} + c, i_2 + 1 \le r \le i_3 - 1, 2^r - 2^{i_1} < c < 2^r$, let $t^{(n)}$ be a 2^n-periodic binary sequence with linear complexity L. Based on Algorithm 2.1.1, after the $n-(r+1)$th step, the period of the sequence $t^{(r+1)}$ becomes 2^{r+1}, the linear complexity of the sequence $t^{(r+1)}$ is c.

Let $u^{(r+1)}$ be a 2^{r+1}-periodic sequence with linear complexity $2^{r+1} - (2^{i_2} + 2^{i_1})$ and $W_H(u^{(r+1)}) = 2^2$. By Theorem 2.7.1, the number of sequences $t^{(r+1)} + u^{(r+1)}$ with linear complexity $2^{r+1} - (2^{i_2} + 2^{i_1})$ is $2^{4r-2i_2-i_1-2} \times 2^{c-1}$.

For any sequence $u^{(r+1)}$, by Theorem 2.7.2, there exists exactly one sequence $v^{(r+1)}$ with linear complexity $2^{r+1} - (2^{i_2} + 2^{i_1})$ and $W_H(u^{(r+1)}) = 2^2$, such that $L(u^{(r+1)} + v^{(r+1)}) = 2^r - (2^{i_2} + 2^{i_1}) < c$.

There exist two sequences $v^{(r+1)}$ with linear complexity $2^{r+1} - (2^{i_2} + 2^{i_1})$ and $W_H(u^{(r+1)}) = 2^2$, such that $L(u^{(r+1)} + v^{(r+1)}) = 2^r - 2^{i_2} < c$.

There exist four sequences $v^{(r+1)}$ with linear complexity $2^{r+1} - (2^{i_2} + 2^{i_1})$ and $W_H(u^{(r+1)}) = 2^2$, such that $L(u^{(r+1)} + v^{(r+1)}) = 2^r - 2^{i_1} < c$.

(The following example is given to illustrate the above case. Suppose that $r + 1 = 4, i_2 = 2, i_1 = 1$, $u^{(r+1)} = \{1010\ 1010\ 0000\ 0000\}$.

Let $v^{(r+1)} = \{0000\ 1010\ 1010\ 0000\}$. Then $u^{(r+1)} + v^{(r+1)} = \{1010\ 0000\ 1010\ 0000\}$. Thus $L(u^{(r+1)} + v^{(r+1)}) = 2^4 - (2^3 + 2^1) = 6$.

Let $v^{(r+1)} = \{1010\ 0000\ 0000\ 1010\}$. Then $u^{(r+1)} + v^{(r+1)} = \{0000\ 1010\ 0000\ 1010\ \}$. Thus $L(u^{(r+1)} + v^{(r+1)}) = 2^4 - (2^3 + 2^1) = 6$.

Let $v^{(r+1)} = \{0010\ 1000\ 1000\ 0010\}$. Then $u^{(r+1)} + v^{(r+1)} = \{1000\ 0010\ 1000\ 0010\ \}$. Thus $L(u^{(r+1)} + v^{(r+1)}) = 2^4 - (2^3 + 2^1) = 6$.

Let $v^{(r+1)} = \{1000\ 0010\ 0010\ 1000\}$. Then $u^{(r+1)} + v^{(r+1)} = \{0010\ 1000\ 0010\ 1000\ \}$. Thus $L(u^{(r+1)} + v^{(r+1)}) = 2^4 - (2^3 + 2^1) = 6$.)

Let $x^{(r+1)} = t^{(r+1)} + u^{(r+1)} + v^{(r+1)}$. Then $L(x^{(r+1)}) = c$, $t^{(r+1)} + u^{(r+1)} = x^{(r+1)} + v^{(r+1)}$. Therefore, the number of distinct sequences $t^{(r+1)} + u^{(r+1)}$ with linear complexity $2^{r+1} - (2^{i_2} + 2^{i_1})$ is

$$2^{4r-2i_2-i_1-2} \times \frac{1}{2^3} \times 2^{c-1}.$$

For a given sequence $t^{(r+1)} + u^{(r+1)}$ with linear complexity $2^{r+1} - (2^{i_2} + 2^{i_1})$, we restore the sequence $t^{(r+1)} + u^{(r+1)}$ to $t^{(n)} + u^{(n)}$ with linear complexity $2^n - (2^{i_m} + 2^{i_{m-1}} + \cdots + 2^{i_1})$ by the reverse process of Algorithm 2.1.1. By Lemma 2.1.5 in Section 2.1, $2^{2^n-(2^{i_m}+2^{i_{m-1}}+\cdots+2^{i_3})-2^{r+1}}$ sequences $t^{(n)} + u^{(n)}$ will be obtained. The number of such sequences $t^{(n)} + u^{(n)}$ is

$$2^{2^n-(2^{i_m}+2^{i_{m-1}}+\cdots+2^{i_3})-2^{r+1}} \times 2^{4r-2i_2-i_1-5} \times 2^{c-1} = 2^{2^n-(2^{i_m}+2^{i_{m-1}}+\cdots+2^{i_3})-2^{r+1}+c+4r-2i_2-i_1-6},$$

where $u^{(n)}$ is a 2^n-periodic binary sequence with linear complexity $2^n - (2^{i_m} + 2^{i_{m-1}} + \cdots + 2^{i_1})$ and $W_H(u^{(n)}) = 2^m$. Also $L_{2^m}(t^{(n)} + u^{(n)}) = 2^n - (2^{i_m} + 2^{i_{m-1}} + \cdots + 2^{i_3}) - 2^{r+1} + c$.

.....

8) Finally, let $t^{(n)}$ be a 2^n-periodic binary sequence with linear complexity $L = 2^n - 2^{r+1} + c, i_m + 1 \leq r < n, 2^r - 2^{i_1} < c < 2^r$. Based on Algorithm 2.1.1, after the $n-(r+1)$th step, the period of the sequence $t^{(r+1)}$ becomes 2^{r+1}, the linear complexity of the sequence $t^{(r+1)}$ is c.

Let $u^{(r+1)}$ be a 2^{r+1}-periodic sequence with linear complexity $2^{r+1} - (2^{i_m} + \cdots + 2^{i_2} + 2^{i_1})$ and $W_H(u^{(r+1)}) = 2^m$. By Theorem 2.7.1, the number of sequences $t^{(r+1)} + u^{(r+1)}$ with linear complexity $2^{r+1} - (2^{i_m} + \cdots + 2^{i_2} + 2^{i_1})$ is $2^{2^m(r+1) - 2^{m-1}i_m - \cdots - 2i_2 - i_1 - 2^{m+1} + 2} \times 2^{c-1}$.

For any sequence $u^{(r+1)}$, by Theorem 2.7.2, there exist $1 + 2 + \cdots + 2^{2^m - 2} = 2^{2^m - 1} - 1$ sequences $v^{(r+1)}$ with linear complexity $2^{r+1} - (2^{i_m} + \cdots + 2^{i_2} + 2^{i_1})$ and $W_H(u^{(r+1)}) = 2^m$, such that $L(u^{(r+1)} + v^{(r+1)}) < c$.

Let $x^{(r+1)} = t^{(r+1)} + u^{(r+1)} + v^{(r+1)}$. Then $L(x^{(r+1)}) = c$, $t^{(r+1)} + u^{(r+1)} = x^{(r+1)} + v^{(r+1)}$. Therefore, the number of distinct sequences $t^{(r+1)} + u^{(r+1)}$ with linear complexity $2^{r+1} - (2^{i_m} + \cdots + 2^{i_2} + 2^{i_1})$ is

$$2^{2^m r - 2^{m-1}i_m - \cdots - 2i_2 - i_1 - 2^m + 2} \times \frac{1}{2^{2^m - 1}} \times 2^{c-1}.$$

For a given sequence $t^{(r+1)} + u^{(r+1)}$ with linear complexity $2^{r+1} - (2^{i_m} + \cdots + 2^{i_2} + 2^{i_1})$, we restore the sequence $t^{(r+1)} + u^{(r+1)}$ to $t^{(n)} + u^{(n)}$ with linear complexity $2^n - (2^{i_m} + 2^{i_{m-1}} + \cdots + 2^{i_1})$ by the reverse process of Algorithm 2.1.1. By Lemma 2.1.5 in Section 2.1, $2^{2^n - 2^{r+1}}$ sequences $t^{(n)} + u^{(n)}$ will be obtained. The number of such sequences $t^{(n)} + u^{(n)}$ is

$$2^{2^n - 2^{r+1}} \times 2^{2^m r - 2^{m-1}i_m - \cdots - 2i_2 - i_1 - 2^{m+1} + 3} \times 2^{c-1} = 2^{2^n - 2^{r+1} + c + 2^m r - 2^{m-1}i_m - \cdots - 2i_2 - i_1 - 2^{m+1} + 2},$$

where $u^{(n)}$ is a 2^n-periodic binary sequence with linear complexity $2^n - (2^{i_m} + 2^{i_{m-1}} + \cdots + 2^{i_1})$ and $W_H(u^{(n)}) = 2^m$. Also $L_{2^m}(t^{(n)} + u^{(n)}) = 2^n - 2^{r+1} + c$.

This completes the proof. □

The above result gives a complete characterization on the first descent point distribution for k-error linear complexity. Several existing results are special cases of Theorem 2.7.4. For $m = 0$, from Theorem 2.7.4, we obtain the following conclusion.

Corollary 3.1 Let $N_1(L)$ be the number of 2^n-periodic binary sequences $s^{(n)}$ with linear

complexity 2^n and 1-error linear complexity L. Then

$$N_1(L) = \begin{cases} 2^n, & L = 0 \\ 2^{L+r}, & L = 2^n - 2^{r+1} + c,\ 1 \le r < n, 1 \le c < 2^r \\ 0, & \text{otherwise} \end{cases}$$

Corollary 3.1 was first proved by Meidl (2005). Here we obtain this result with a different approach.

For $m = 1, i_1 = 0$, from Theorem 2.7.4, it is easy to verify the following conclusion, which was first proved by Zhu and Qi (2007).

Corollary 3.2 Let $N_2(L)$ be the number of 2^n-periodic binary sequences $s^{(n)}$ with linear complexity $2^n - 1$ and the 2-error linear complexity L. Then

$$N_2(L) = \begin{cases} 2^{2n-2}, & L = 0 \\ 2^{L+2r-1}, & L = 2^n - 2^{r+1} + c,\ 2 \le r < n, 1 \le c < 2^r - 1 \\ 0, & \text{otherwise} \end{cases}$$

For $m = 2$, the main result by Pi and Qi (2011) is also a special case of Theorem 2.7.4.

2.8 Summary

In this chapter, we proposed a unified framework for the k-error linear complexity distribution of 2^n-periodic binary sequences, and completely solved the problem of 2-error, 3-error and 4-error linear complexity distribution of 2^n periodic binary sequences. One can see that the decomposition in the case of 4-error is much more complicated than that of 2-error and 3-error. As to the case of the 5-error linear complexity, we only obtained partial results in this chapter and for complete solution, it remains to study the case that $w^{(n)} = u^{(n)} + v^{(n)}$, with $W(u^{(n)}) = 3$ or 5, $W(v^{(n)}) = 3$ or 5, $L(w^{(n)}) = 2^{n-1} - 2^{d_1} - 2^{d_2}$ and $W(w^{(n)}) = 8$. The key issue in the problem is that $W(w^{(n)})$ is still 8. In this case, we need to calculate its different possible combinations. However, this is not an easy task currently. We expect that with the technique of sequence decomposition proposed in this chapter, one can obtain the complete counting functions for the 5-error linear complexity distribution. We will continue this work in future due to its importance.

Of course, we can consider the 6-error linear complexity and the 7-error linear complexity with the proposed approach in this chapter and obtain some partial results similar to the

case of $k = 5$. As to the difficulty of this problem in nature, we will do it in future as we believe the proposed approach can pave a way for their complete solutions. One can imagine that the decomposition will become more and more complicated when the value k increases.

Chapter 3

Cube Theory and Stable k-error Linear Complexity

The motivation of studying the stability of linear complexity is that changing a small number of elements in a sequence may lead to a sharp decline of its linear complexity. Therefore we really need to study such stable sequences in which even a small number of changes do not reduce their linear complexity. The stable k-error linear complexity is introduced in this chapter to deal with this problem. Suppose that s is a sequence over $GF(q)$ with period N. For $k(0 \leq k \leq N)$, the k-error linear complexity of s is defined as stable when any k or fewer of the terms of the sequence are changed within one period, the linear complexity does not decline.

Algebra (Meidl, 2004, 2005; Fu *et al.*, 2006; Zhu and Qi, 2007) and discrete Fourier transform (Hu and Feng, 2005) are two important tools to study the k-error linear complexity for periodic sequences. Etzion *et al.* (2009) studied the sequences with only two k-error linear complexity values exactly, namely its k-error linear complexity is only $L(s)$ or 0. To further investigate this concept, we present a new tool called the **Cube Theory** (Zhou *et al.*, 2013) to study the stable k-error linear complexity of binary sequences with period 2^n. By using the cube theory, we are capable of investigating the k-error linear complexity for periodic sequences from a new perspective. First, one significant benefit is that one can construct sequences with the maximum stable k-error linear complexity. Some examples are also given to illustrate the proposed approach. Second, it is proved that a binary sequence with period 2^n can be decomposed into some disjoint cubes. Based on the Games-Chan Algorithm, we further propose **a standard cube decomposition** for any binary sequence with period 2^n. The main approaches of Chapter 4 and Chapter 5 are based on the cube decomposition theory. With such decomposition, it is proved that the maximum k-error linear complexity is $2^n - (2^l - 1)$ over all 2^n-periodic binary sequences, where $2^{l-1} \leq k < 2^l$. As a consequence of these results, some results by Niu *et al.* (2013, 2014) are proved to be incorrect. Finally, continuing the work of Kurosawa *et al.* (2000) with different approaches, a characterization is presented about the minimum number k for which the second decrease occurs in the k-error linear complexity.

The rest of this chapter is organized as follows. In Section 3.1, some preliminary results are presented. In Section 3.2, the definition of cube theory and our main results are presented.

3.1 Preliminaries

The linear complexity of a 2^n-periodic binary sequence s can be recursively computed by the Games-Chan algorithm (Games and Chan, 1983) stated as follows.

Algorithm 3.1.1

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 $Left(s) \bigoplus Right(s)$ recursively. Namely, $L(s) = 2^{n-1} + L(Left(s) \bigoplus Right(s))$.

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

From Lemma 2.1.1 in Section 2.1, if a nonzero element is changed to zero 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.

Suppose that the linear complexity of s can decrease when at least k elements of s are changed. By Lemma 2.1.2 in Section 2.1, the linear complexity of the binary sequence, in which elements at exactly those k positions are all nonzero, must be $L(s)$. Therefore, for the computation of the k-error linear complexity, we only need to find the binary sequence whose Hamming weight achieves the minimum and its linear complexity is $L(s)$.

Denote E_{ij} by a binary sequence with period 2^n, and it has only 2 nonzero elements in a period. By Lemma 2.1.3 in Section 2.1, if there are only 2 adjacent positions with nonzero elements in E_{ij}, then its linear complexity is $2^n - 1$, namely E_{ij} is a sequence with even Hamming weight and the largest linear complexity. According to Lemma 2.1.2 in Section

2.1, if sequence s can be decomposed into the superposition of several E_{ij}s, in which each has linear complexity $2^n - 1$, and the number of E_{ij}s is odd, then $L(s) = 2^n - 1$. After a symbol of s is changed, its Hamming weight will be odd, so its linear complexity will be 2^n, namely the 1-error linear complexity of sequence s is $2^n - 1$.

Proposition 3.1.1 If s is a binary sequence with period 2^n, then its maximum 1-error linear complexity is $2^n - 1$.

In order to discuss the maximal 2-error linear complexity of a binary sequence with period 2^n, we now consider a binary sequence which has only 4 positions with nonzero elements.

Lemma 3.1.1 If s is a 2^n-periodic binary sequence and there are only four non-zero elements, thus s can be decomposed into the superposition of E_{ij} and E_{kl}, where $i < j, i < k < l$. If d, e are the largest integers satisfying $i \equiv j(\mod 2^d)$, $k \equiv l(\mod 2^e)$, and $k - i \equiv 1(\mod 2)$ separately, then

$$L(s) = \begin{cases} 2^n - (1 + 2^d), & \text{if } e = d \\ 2^n - 2^{\min(d,e)}, & \text{otherwise} \end{cases}$$

Proof. According to Lemma 2.1.2 in Section 2.1, if $d \neq e$, then $L(s) = 2^n - 2^{\min(d,e)}$.

Consider the case of $d = e$. Denote E_i by a binary sequence with period 2^n, and it has only one nonzero element with index i in a period. We know that s can be decomposed into the sum of E_i, E_j, E_k and E_l. The corresponding polynomial of $E_i + E_j$ is given by

$$\begin{aligned} x^i + x^j &= x^i(1 - x^{j-i}) = x^i(1 - x^{2^d(1+2u)}) \\ &= x^i(1 - x^{2^d})(1 + x^{2^d} + x^{2\cdot 2^d} + \cdots + x^{2u\cdot 2^d}) \end{aligned}$$

where u is a positive integer. The corresponding polynomial of $E_k + E_l$ is given by

$$\begin{aligned} x^k + x^l &= x^k(1 - x^{l-k}) = x^k(1 - x^{2^d(1+2v)}) \\ &= x^k(1 - x^{2^d})(1 + x^{2^d} + x^{2\cdot 2^d} + \cdots + x^{2v\cdot 2^d}) \end{aligned}$$

where v is a positive integer. Then $E_i + E_j + E_k + E_l$ corresponds to a polynomial, which

is given by

$$\begin{aligned}
& x^i + x^j + x^k + x^l \\
= \; & x^i(1-x^{2^d})[(1+x^{2^d}+x^{2\cdot 2^d}+\cdots+x^{2u\cdot 2^d}) \\
& \quad +x^{k-i}(1+x^{2^d}+x^{2\cdot 2^d}+\cdots+x^{2v\cdot 2^d})] \\
= \; & x^i(1-x^{2^d})[1+x^{k-i}+(x^{2^d}+x^{2\cdot 2^d}+\cdots+x^{2u\cdot 2^d}) \\
& \quad +x^{k-i}(x^{2^d}+x^{2\cdot 2^d}+\cdots+x^{2v\cdot 2^d})] \\
= \; & x^i(1-x^{2^d})[1+x^{2c+1}+(x^{2^d}+x^{2\cdot 2^d}+\cdots+x^{2u\cdot 2^d}) \\
& \quad +x^{k-i}(x^{2^d}+x^{2\cdot 2^d}+\cdots+x^{2v\cdot 2^d})] \\
= \; & x^i(1-x)^{2^d+1}[(1+x+x^2+\cdots+x^{2c}) \\
& \quad +(x^{2^d}+x^{3\cdot 2^d}+\cdots+x^{(2u-1)\cdot 2^d})(1+x)^{2^d-1} \\
& \quad +x^{k-i}(x^{2^d}+x^{3\cdot 2^d}+\cdots+x^{(2v-1)\cdot 2^d})(1+x)^{2^d-1}]
\end{aligned}$$

where c is a positive integer. Since there is no factor $(1+x)$ in $(1+x+x^2+\cdots+x^{2c})$, hence $\gcd((1-x)^{2^n}, x^i+x^j+x^k+x^l) = (1-x)^{2^d+1}$, thus, $L(s) = 2^n - (2^d+1)$.

This completes the proof. □

More specifically, we have the following result.

Lemma 3.1.2 If s is a binary sequence with period 2^n and there are only 4 non-zero elements, and s can be decomposed into the superposition of E_{ij} and E_{kl}, in which each has linear complexity 2^n-1, then the linear complexity of s is $2^n-(2^d+1)$ or $2^n-2^d, d>0$.

Proof. Suppose that the non-zero positions of E_{ij} are i and j, whose linear complexity is $2^n-1, j-i=2a+1$, and non-zero positions of E_{kl} are k and l, whose linear complexity is also 2^n-1, $i<k, l-k=2b+1$.

Next we will investigate the problem with the following 6 cases:

1) $i<k<l<j$, and $k-i=2c$.

As $j-i=2a+1, l-k=2b+1$, so

$$j-l = 2a+1-(2b+1+2c) = 2(a-b-c)$$

.

If $j-l=2^d+2u2^d, k-i=2^e+2v2^e$, without loss of generality, assume $d<e$, by Lemma 2.1.2 in Section 2.1, $L(s)=2^n-2^d$, $d>0$.

If $d=e$, by Lemma 3.1.1, since $l-i=2(b+c)+1$, so $L(s)=2^n-(2^d+1)$.

2) $i<k<l<j$, and $k-i=2c+1$.

As $j-i=2a+1, l-k=2b+1$, so $l-i=2b+1+2c+1=2(b+c+1), j-k=2a+1-(2c+1)=2(a-c)$

If $j-k=2^d+2u2^d, l-i=2^e+2v2^e$, without loss of generality, assume $d<e$, by Lemma 2.1.2 in Section 2.1, $L(s)=2^n-2^d$, $d>0$.

Since $k-i=2c+1$, by Lemma 3.1.1, if $d=e$, then $L(s)=2^n-(2^d+1)$.

3) $i<k<j<l$, and $k-i=2c$.

As $j-i=2a+1, l-k=2b+1$,so $j-k=2a+1-2c=2(a-c)+1, l-j=2b+1-[2(a-c)+1]=2(b+c-a)$

If $l-j=2^d+2u2^d, k-i=2^e+2v2^e$, without loss of generality, assume $d<e$, by Lemma 2.1.2 in Section 2.1, $L(s)=2^n-2^d, d>0$.

Since $j-i=2a+1$, by Lemma 3.1.1, if $d=e$, then $L(s)=2^n-(2^d+1)$.

4) $i<k<j<l$, and $k-i=2c+1$.

As $j-i=2a+1, l-k=2b+1$,so $j-k=2a+1-(2c+1)=2(a-c), l-i=2b+1+2c+1=2(b+c+1)$.

If $l-i=2^d+2u2^d, j-k=2^e+2v2^e$, without loss of generality, assume $d<e$, by Lemma 2.1.2 in Section 2.1,$L(s)=2^n-2^d$,$d>0$.

Since $k-i=2c+1$, by Lemma 3.1.1, if $d=e$, then $L(s)=2^n-(2^d+1)$.

5) $i<j<k<l$, and $k-i=2c$.

As $j-i=2a+1, l-k=2b+1$, so $k-j=2c-(2a+1)=2(c-a)-1, l-j=2b+1+[2(c-a)-1]=2(b+c-a)$

If $l-j=2^d+2u2^d, k-i=2^e+2v2^e$, without loss of generality, assume $d<e$, by Lemma 2.1.2 in Section 2.1, $L(s)=2^n-2^d, d>0$.

Note that $j-i=2a+1$, by Lemma 3.1.1, if $d=e$, then $L(s)=2^n-(2^d+1)$.

6) $i<j<k<l$, and $k-i=2c+1$.

As $j-i=2a+1, l-k=2b+1$, so $k-j=2c+1-(2a+1)=2(c-a), l-i=2b+1+2c+1=2(b+c+1)$

If $l-i=2^d+2u2^d, k-j=2^e+2v2^e$, without loss of generality, assume $d<e$, by Lemma 2.1.2 in Section 2.1, $L(s)=2^n-2^d, d>0$.

Note that $k-i=2c+1$, by Lemma 3.1.1, if $d=e$, then $L(s)=2^n-(2^d+1)$.

Based on the above 6 cases, we conclude that the lemma can be established. □

Corollary 3.1.1 Suppose that s is a binary sequence with period 2^n and there are only 4 non-zero elements, and s can be decomposed into the superposition of E_{ij} and E_{kl}. If non-zero positions of E_{ij} are i and $j, j-i$ is an odd number, and non-zero positions of E_{kl} are k and $l, l-k$ is also an odd number, and $i<k, k-i=4c+2, |l-j|=4d+2$, or $|k-j|=4c+2, |l-i|=4d+2$, then the linear complexity of s is 2^n-3.

Proof. According to case 1), 3) and 5) of Lemma 3.1.2, if $k-i=4c+2, |l-j|=4d+2$, then $|l-j|=2+4d, k-i=2+4c$. By Lemma 3.1.1, noting that $j-i=2a+1$, so $L(s)=2^n-(2+1)$.

According to case 2), 4) and 6) of Lemma 3.1.2, if $|k-j|=4c+2, |l-i|=4d+2$, then it is easy to know that $k-i$ is odd, thus $|k-j|=2+4c, |l-i|=2+4d$. By Lemma 3.1.1, $L(s)=2^n-(2+1)$. □

Corollary 3.1.2 If s is a binary sequence with period 2^n and there are only 4 non-zero elements, and s can be decomposed into the sum of two E_{ij}, in which each has linear complexity 2^n-2, then the linear complexity of s is $2^n-(2+1)$ or $2^n-(2^d+1)2, d>0$ or $2^n-2^d, d>1$.

Proof. Suppose that non-zero positions of the first E_{ij} are i and j, $j-i=4a+2$, and

non-zero positions of the second E_{ij} are k and $l, l-k=4b+2$, where $i<k$.

If $k-i=2c+1$, according to Lemma 3.1.1, then $L(s)=2^n-(2+1)$.

If $k-i=2c$, the corresponding polynomial of $E_i+E_j+E_k+E_l$ is given by

$x^i+x^j+x^k+x^l=x^i(1+x^{j-i}+x^{k-i}+x^{l-k+k-i})$

Therefore, we only need to consider

$1+x^{j-i}+x^{k-i}+x^{l-k+k-i}=1+(x^2)^{2a+1}+(x^2)^c+(x^2)^{2b+1+c}=1+y^{2a+1}+y^c+y^{2b+1+c}$

According to Lemma 3.1.2, $L(s)=2^n-(2^d+1)2, d>0$ or $2^n-2^d, d>1$. □

Now we can obtain the following conclusions according to Lemma 3.1.2 and Corollary 3.1.2.

Proposition 3.1.2 Suppose that s is a binary sequence with period 2^n and there are four non-zero elements, then the necessary and sufficient conditions for the linear complexity of s being 2^n-3 are given by: s can be decomposed into the superposition of E_{ik} and E_{jl}, in which each has linear complexity 2^n-2. Further, if the non-zero positions of E_{ik} are i and k, with $k-i=4c+2$, and the non-zero positions of the second E_{jl} are j and l, with $l-j=4d+2$, where $i<j$, then $j-i=2a+1$(or $|l-k|=2b+1$ or $|l-i|=2e+1$ or $|k-j|=2f+1$).

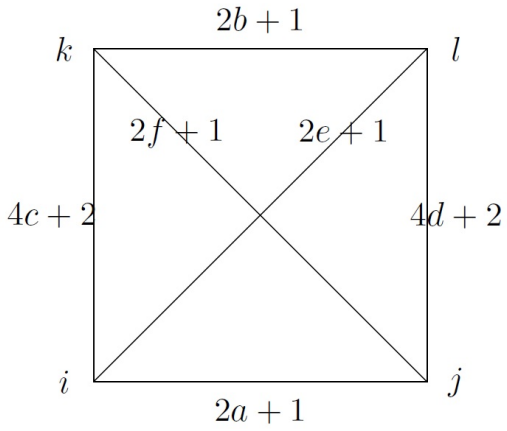

Figure 3.1: A graphic illustration of Proposition 3.1.2

We can also illustrate this with a graph in Figure 3.1. The only 4 non-zero positions of

sequence s are i, j, k and l. As $k - i = 4c + 2$, $l - j = 4d + 2$, and $j - i = 2a + 1$, so $l - k = l - j + j - i - (k - i) = 4d + 2 + 2a + 1 - (4c + 2)$ is odd. Next we give a result on the stable sequence.

Proposition 3.1.3 Suppose that s is a binary sequence with period 2^n and its Hamming weight is even, then the maximum stable 2-error linear complexity of s is $2^n - 3$.

Proof. Assume that $L(s) = 2^n - 1$, then s can be decomposed into the sum of several E_{ij}s and the number of E_{ij}s with linear complexity $2^n - 1$ is odd. According to Lemma 2.1.2 in Section 2.1, if an E_{ij} with linear complexity $2^n - 1$ is removed, then the linear complexity of s will be less than $2^n - 1$, namely the 2-error linear complexity of s is less than $2^n - 1$.

Assume that $L(s) = 2^n - 2$, then s can be decomposed into the sum of several E_{ij}s and the number of E_{ij}s with linear complexity $2^n - 2$ is odd. If an E_{ij} with linear complexity $2^n - 2$ is removed, then the linear complexity of s will be less than $2^n - 2$, namely the 2-error linear complexity of s is less than $2^n - 2$.

Assume that $L(s) = 2^n - 3$, without loss of generality, here we only discuss the case that s has 4 non-zero elements: e_i, e_j, e_k and e_l, and $L(E_i + E_j + E_k + E_l) = 2^n - 3$. If any two of them are removed, by Proposition 3.1.2, the linear complexity of remaining elements of the sequence is $2^n - 1$ or $2^n - 2$. From Figure 3.1, after e_i and e_l are changed to zero, we can see that the linear complexity of the sequence composed by e_j and e_k is $2^n - 1$.

If the position of one element from e_i, e_j, e_k and e_l is changed, then there exist two elements, of which the position difference remains unchanged as odd, thus $L(s) \geq 2^n - 3$.

If two nonzero elements are added to the position outside e_i, e_j, e_k and e_l, namely an E_{ij} with linear complexity $2^n - 2^d$ is added to sequence s, according to Lemma 2.1.2 in Section 2.1, the linear complexity will be $2^n - 1$, $2^n - 2$ or $2^n - 3$.

Summarizing all above discussions, the proof is completed. □

The following is an example to illustrate Proposition 3.1.3.

The linear complexity of $11110 \cdots 0$ is $2^n - 3$

The linear complexity of $01010 \cdots 0$ or $10100 \cdots 0$ is $2^n - 2$

The linear complexity of $01100\cdots0$ or $10010\cdots0$ is 2^n-1

If two additional nonzero elements are added to $11110\cdots0$, namely an E_{ij} whose linear complexity is 2^n-2^d is added to it, according to Lemma 2.1.2 in Section 2.1, the linear complexity will become 2^n-1, 2^n-2 or 2^n-3.

For instance, suppose that $1110\cdots010\cdots0$ is the addition of $11110\cdots0$ and $0001\cdots010\cdots0$. We here only consider the case that the position difference of the last two nonzero elements is $2c+1$. According to case 5) of Lemma 3.1.2, $j-i=1, l-k=2c+1$, so $k-j=1, l-j=2(c+1)$.

Noticed that $k-i=2$, if $l-j=2^d(2u+1)$, according to Lemma 2.1.2 in Section 2.1, $L(s)=2^n-2$ when $d>1$.

If $d=1$, since $j-i=1$, according to Lemma 3.1.1, $L(s)=2^n-3$.

3.2 The Cube Theory and Main Results

Before presenting main results, we first consider a special case.

Lemma 3.2.1 Suppose that s is a binary sequence with period 2^n and there are 8 non-zero elements, thus s can be decomposed into the superposition of E_{ij}, E_{kl}, E_{mn} and E_{pq}. Suppose that non-zero positions of E_{ij} are i and $j, j-i=2a+1$, and non-zero positions of E_{kl} are k and $l, l-k=2b+1$, and $k-i=4c+2, l-j=4d+2$, and non-zero positions of E_{mn} are m and n, non-zero positions of E_{pq} are p and q, and $m-i=4+8u, n-j=4+8v, p-k=4+8w, q-l=4+8y$, where a, b, c, d, u, v, w and y are all non-negative integers, then the linear complexity of s is 2^n-7.

Proof. According to Corollary 3.1.1, $L(E_i+E_j+E_k+E_l)=2^n-3$.

As $m-n=m-i-(n-j)-(j-i)$, $p-q=p-k-(q-l)-(l-k)$, thus both $m-n$ and $p-q$ are odd numbers.

As $p-m=p-k-(m-i)+(k-i)$, $q-n=q-l-(n-j)+(l-j)$, thus both $p-m$ and $q-n$ are multiples of 2, but not multiples of 4. According to Corollary 3.1.1, $L(E_m+E_n+E_p+E_q)=2^n-3$.

Similar to the proof of Lemma 3.1.1, the corresponding polynomial of $E_i + E_k + E_m + E_p$ is given by

$$\begin{aligned}
& x^i + x^k + x^m + x^p \\
= \; & x^i(1-x^4)[(1 + x^4 + x^{2\cdot 4} + \cdots + x^{2u\cdot 4}) \\
& \quad + x^{k-i}(1 + x^4 + x^{2\cdot 4} + \cdots + x^{2w\cdot 4})] \\
= \; & x^i(1-x^4)[1 + x^{k-i} + (x^4 + x^{2\cdot 4} + \cdots + x^{2u\cdot 4}) \\
& \quad + x^{k-i}(x^4 + x^{2\cdot 4} + \cdots + x^{2w\cdot 4})] \\
= \; & x^i(1-x^4)[1 + x^{4c+2} + (x^4 + x^{2\cdot 4} + \cdots + x^{2u\cdot 4}) \\
& \quad + x^{k-i}(x^4 + x^{2\cdot 4} + \cdots + x^{2w\cdot 4})] \\
= \; & x^i(1-x)^6[(1 + x^2 + x^4 + \cdots + x^{4c}) \\
& \quad + (x^4 + x^{3\cdot 4} + \cdots + x^{(2u-1)\cdot 4})(1+x)^2 \\
& \quad + x^{k-i}(x^4 + x^{3\cdot 4} + \cdots + x^{(2w-1)\cdot 4})(1+x)^2]
\end{aligned}$$

The corresponding polynomial of $E_j + E_l + E_n + E_q$ is given by

$$\begin{aligned}
& x^j + x^l + x^n + x^q \\
= \; & x^j(1-x^4)[(1 + x^4 + x^{2\cdot 4} + \cdots + x^{2v\cdot 4}) \\
& \quad + x^{l-j}(1 + x^4 + x^{2\cdot 4} + \cdots + x^{2y\cdot 4})] \\
= \; & x^j(1-x)^6[(1 + x^2 + x^4 + \cdots + x^{4d}) \\
& \quad + (x^4 + x^{3\cdot 4} + \cdots + x^{(2v-1)\cdot 4})(1+x)^2 \\
& \quad + x^{l-j}(x^4 + x^{3\cdot 4} + \cdots + x^{(2y-1)\cdot 4})(1+x)^2]
\end{aligned}$$

The corresponding polynomial of $E_i + E_j + E_k + E_l + E_m + E_n + E_p + E_q$ is given by

$$\begin{aligned}
& x^i + x^j + x^k + x^l + x^m + x^n + x^p + x^q \\
= \; & x^i(1-x)^6\{(1 + x^2 + x^4 + \cdots + x^{4c}) \\
& +(x^4 + x^{3\cdot 4} + \cdots + x^{(2u-1)\cdot 4})(1+x)^2 \\
& +x^{k-i}(x^4 + x^{3\cdot 4} + \cdots + x^{(2w-1)\cdot 4})(1+x)^2 \\
& +x^{j-i}[(1 + x^2 + x^4 + \cdots + x^{4d}) \\
& +(x^4 + x^{3\cdot 4} + \cdots + x^{(2v-1)\cdot 4})(1+x)^2 \\
& +x^{l-j}(x^4 + x^{3\cdot 4} + \cdots + x^{(2y-1)\cdot 4})(1+x)^2]\} \\
= \; & x^i(1-x)^6\{1 + x^{j-i} + (x^2 + x^4 + \cdots + x^{4c}) \\
& +(x^4 + x^{3\cdot 4} + \cdots + x^{(2u-1)\cdot 4})(1+x)^2 \\
& +x^{k-i}(x^4 + x^{3\cdot 4} + \cdots + x^{(2w-1)\cdot 4})(1+x)^2 \\
& +x^{j-i}[(x^2 + x^4 + \cdots + x^{4d}) \\
& +(x^4 + x^{3\cdot 4} + \cdots + x^{(2v-1)\cdot 4})(1+x)^2 \\
& +x^{l-j}(x^4 + x^{3\cdot 4} + \cdots + x^{(2y-1)\cdot 4})(1+x)^2]\} \\
= \; & x^i(1-x)^7\{1 + x + x^2 + \cdots + x^{2a} \\
& +x^2(1+x)(1 + x^4 + \cdots + x^{4(c-1)}) \\
& +(x^4 + x^{3\cdot 4} + \cdots + x^{(2u-1)\cdot 4})(1+x) \\
& +x^{k-i}(x^4 + x^{3\cdot 4} + \cdots + x^{(2w-1)\cdot 4})(1+x) \\
& +x^{j-i}[x^2(1+x)(1 + x^4 + \cdots + x^{4(d-1)}) \\
& +(x^4 + x^{3\cdot 4} + \cdots + x^{(2v-1)\cdot 4})(1+x) \\
& +x^{l-j}(x^4 + x^{3\cdot 4} + \cdots + x^{(2y-1)\cdot 4})(1+x)]\}
\end{aligned}$$

The number of items in $(1 + x + x^2 + \cdots + x^{2a})$ is odd, thus there is no factor $(1 + x)$ in $(1 + x + x^2 + \cdots + x^{2a})$. Thus we have

$$\gcd((1-x)^{2^n}, x^i + x^j + x^k + x^l + x^m + x^n + x^p + x^q) = (1-x)^7$$

It is followed by $L(s) = 2^n - 7$. □

For the convenience of presentation, we introduce some definitions.

Definition 3.2.1 Suppose that the difference of positions (or indexes) of two non-zero elements of sequence s is $(2x + 1)2^y$, both x and y are non-negative integers, then the

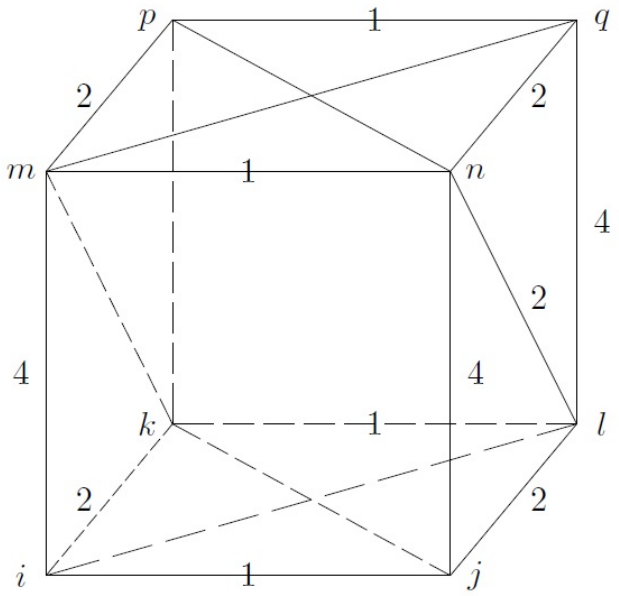

Figure 3.2: A graphic illustration of Lemma 3.2.1

distance between the two elements is defined as 2^y.

Definition 3.2.2 Suppose that s is a binary sequence with period 2^n, and there are 2^m non-zero elements in s, and $0 \leq i_1 < i_2 < \cdots < i_m < n$. If $m = 1$, then there are 2 non-zero elements in s and the distance (based on Definition 3.2.1 above) 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 3.2.3 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.

Now we consider the linear complexity of a cube.

Theorem 3.2.1 Suppose that s is a binary sequence with period 2^n, and non-zero elements of s form a m-cube, if lengths of edges are $i_1, i_2, \cdots, i_m$ $(0 \leq i_1 < i_2 < \cdots < i_m < n)$

respectively, then $L(s) = 2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m})$.

Proof. Similar to the proof of Lemma 3.2.1, it is easy to prove Theorem 3.2.1 with mathematical induction.

Based on the Games-Chan algorithm (Games and Chan, 1983), we give another proof from different perspective.

In the kth step, $1 \leq k \leq n$, if and only if one period of the sequence can not be divided into two equal parts, then the linear complexity should be increased by half period. In the kth step, the linear complexity can be increased by maximum 2^{n-k}.

Suppose that non-zero elements of sequence s form a m-cube, lengths of edges are $i_1, i_2, \cdots, i_m$ $(0 \leq i_1 < i_2 < \cdots < i_m < n)$ respectively. Then in the $(n - i_m)$th step, one period of the sequence can be divided into two equal parts, then the linear complexity should not be increased by 2^{i_m}.

.....

In the $(n - i_2)$th step, one period of the sequence can be divided into two equal parts, then the linear complexity should not be increased by 2^{i_2}.

In the $(n - i_1)$th step, one period of the sequence can be divided into two equal parts, then the linear complexity should not be increased by 2^{i_1}.

Therefore, $L(s) = 1+1+2+2^2+\cdots+2^{n-1}-(2^{i_1}+2^{i_2}+\cdots+2^{i_m}) = 2^n-(2^{i_1}+2^{i_2}+\cdots+2^{i_m})$.

The proof is complete now. □

There is a 3-cube in Figure 3.2. $L(s) = 2^n - (1 + 2 + 4)$, and lengths of edges are $1, 2$ and 4 respectively. Next we give a decomposition result.

Theorem 3.2.2 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 $0 \leq i_1 < i_2 < \cdots < i_m < n$, then the sequence s can be decomposed into several disjoint cubes, and only one cube has the linear complexity $2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m})$, other cubes possess distinct linear complexity which are all less than $2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m})$. If the sequence s consists of only one cube, then the Hamming weight of s is 2^m.

Proof. The mathematical induction will be applied to the degree d of $s^N(x)$. For $d < 3$, by Lemma 2.1.3 in Section 2.1, the theorem is obvious.

We first consider a simple case.

A) Suppose that $L(s) = 2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m} + 2^{i_{m+1}})$, and the Hamming weight of s is the minimum, namely $L(s) \neq 2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m} + 2^{i_{m+1}})$ when we remove 2 or more non-zero elements. Next we prove that s consists of one $(m+1)$-cube exactly. Let

$$\begin{aligned} s^N(x) &= (1 - x^{2^{i_1}})(1 - x^{2^{i_2}}) \cdots (1 - x^{2^{i_m}})(1 - x^{2^{i_{m+1}}}) \\ &\quad [1 + f(x)(1 - x)] \end{aligned}$$

Then $t^N(x) = (1 - x^{2^{i_1}})(1 - x^{2^{i_2}}) \cdots (1 - x^{2^{i_m}})[1 + f(x)(1 - x)]$ corresponds to a sequence t whose linear complexity is $L(t) = 2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m})$. The degree of $t^N(x)$ is less than the degree of $s^N(x)$, so the mathematical induction can be applied.

In the following, we consider two cases. We will prove that the second case is equivalent to the first case.

1) The Hamming weight of sequence t is 2^m. By mathematical induction, t is an m-cube. Since $s^N(x) = t^N(x)(1 - x^{2^{i_{m+1}}}) = t^N(x) + x^{2^{i_{m+1}}} t^N(x)$, and $0 \leq i_1 < i_2 < \cdots < i_m < i_{m+1} < n$, so s is a $(m+1)$-cube and its Hamming weight is 2^{m+1}.

2) The Hamming weight of sequence t is $2^m + 2y$. By mathematical induction, the sequence t can be decomposed into several disjoint cubes, and only one cube has the linear complexity $2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m})$. Thus

$t^N(x) = (1 - x^{2^{i_1}})(1 - x^{2^{i_2}}) \cdots (1 - x^{2^{i_m}})[1 + g(x)(1 - x) + h(x)(1 - x)]$, and $u^N(x) = (1 - x^{2^{i_1}})(1 - x^{2^{i_2}}) \cdots (1 - x^{2^{i_m}})[1 + g(x)(1 - x)]$, corresponds to an m-cube, its non-zero elements form a set denoted by A.

$v^N(x) = (1 - x^{2^{i_1}})(1 - x^{2^{i_2}}) \cdots (1 - x^{2^{i_m}})h(x)(1 - x)$ corresponds to several cubes, whose 2y non-zero elements form a set denoted by B.

Assume that $b \in B, bx^{2^{i_{m+1}}} \in A$, we swap b and $bx^{2^{i_{m+1}}}$, namely let $b \in A, bx^{2^{i_{m+1}}} \in B$. It is easy to show that the linear complexity of the sequence to which $u^N(x)$ corresponds remains unchanged. The new $u^N(x)$ is still an m-cube.

$s^N(x) = t^N(x)(1 - x^{2^{i_{m+1}}}) = u^N(x) + v^N(x) - u^N(x)x^{2^{i_{m+1}}} - v^N(x)x^{2^{i_{m+1}}}$, $u^N(x)x^{2^{i_{m+1}}}$ corresponds to 2^m non-zero elements which form a set denoted by C. $v^N(x)x^{2^{i_{m+1}}}$ corresponds to 2y non-zero elements which form a set denoted by D.

By definition, set A and set C disjoint, set B and set D disjoint.

Suppose that set A and set D intersects. Thus there exists $b \in B$, such that $bx^{2^{i_{m+1}}} \in A$, which contradicts the assumption that $b \in A, bx^{2^{i_{m+1}}} \in B$. So set A and set D disjoint.

As set A and set B disjoint, we know that set C and set D disjoint.

We now prove that Set C and B disjoint by contradiction approach.

Suppose that $b \in B, b = ax^{2^{i_{m+1}}} \in C, a \in A$, then $ax^{2(2^{i_{m+1}})}$ must be in D, so sequence s has non-zero elements a and $ax^{2(2^{i_{m+1}})}$. The linear complexity of the sequence with only non-zero elements a and $ax^{2(2^{i_{m+1}})}$ is

$$2^n - 2 \cdot 2^{i_{m+1}} < 2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m} + 2^{i_{m+1}}).$$

Based on Lemma 2.1.2 in Section 2.1, if the two non-zero elements are changed to zero, the linear complexity of s remains unchanged. This contradicts the assumption that the Hamming weight is the minimum, so A and C form a $(m+1)$-cube exactly, and its linear complexity is $2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m} + 2^{i_{m+1}})$.

By the assumption of Case A), s has the minimum Hamming weight, so s consists of a $(m+1)$-cube exactly.

B) Let $s^N(x) = u^N(x) + v^N(x)$, where the Hamming weight of $u^N(x)$ is the minimum, and

$$L(u) = 2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m} + 2^{i_{m+1}}).$$

From Case A), $u^N(x)$ consists of a $(m+1)$-cube exactly.

Let $v^N(x) = y^N(x) + z^N(x)$, where the Hamming weight of $y^N(x)$ is minimum, and $L(y) = L(v)$. By Case A), $y^N(x)$ consists of only one cube exactly. By analogy, we can prove that s consists of several cubes, and only one cube has the linear complexity of $2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m} + 2^{i_{m+1}})$, other cubes possess distinct linear complexity which are all less than $2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m} + 2^{i_{m+1}})$.

This completes proof. □

The following examples can help us understand the proof of Theorem 3.2.2.

$(1+x)(1+x^2)[1+x^5(1+x^2)] = 1+x+x^2+x^3+x^5+x^6+x^9+x^{10}$ corresponds to a sequence in which there are 8 non-zero elements. It consists of two 2-cubes: $(1+x)(1+x^2)$ and $(1+x)(1+x^4)x^5$.

$(1+x)(1+x^2)[1+x^5(1+x^2)](1+x^4) = 1+x+x^2+x^3+x^4+x^7+x^{13}+x^{14}$ corresponds to a sequence in which there are also 8 non-zero elements, but only one 3-cube. The linear complexity is $2^n-(1+2+4)$, and the lengths of edges are 1, 2 and 4 respectively.

Based on Algorithm 3.1.1, we may have a standard cube decomposition for any binary sequence with period 2^n and $L(s) < 2^n$ (Zhou *et al.*, 2015b).

Algorithm 3.2.1

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

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 $Left(s^{(n)}) \bigoplus Right(s^{(n)})$. 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, one can achieve $Left(s^{(n)}) = Right(s^{(n)})$. In this case, we obtain a cube c_1 with linear complexity $L(s^{(n)})$.

Step 5. With $s^{(n)} \bigoplus c_1$, 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 $s^{(n)}$. One can observe that cube decomposition of a sequence may not be unique in general, but **the standard cube decomposition** of a

sequence is unique.

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 $Left \bigoplus Right$. Then the cube $1 + x^8$ is removed.

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

Suppose that the linear complexity of s can reduce when at least k elements of s are changed. By Lemma 2.1.2 in Section 2.1, 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 3.2.1 and Theorem 3.2.2, it is easy to achieve the following conclusion.

Corollary 3.2.1 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 $0 \leq i_1 < i_2 < \cdots < i_m < n$. If $k_{\min}$ is the minimum, such that the $k_{\min}$-error linear complexity is less than $L(s)$, then $k_{\min} = 2^m$.

Corollary 3.2.1 was first proved by Kurosawa *et al.* (2000), and later it was proved by Etzion *et al.* (2009) with a different approach.

Obviously, previous Proposition 3.1.2 and Proposition 3.1.3 are also corollaries of Theorem 3.2.1 and Theorem 3.2.2.

Now we 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 3.2.1 and Theorem 3.2.2, we can obtain the following results on stability.

Corollary 3.2.2 Suppose that s is a binary sequence with period 2^n and its Hamming weight is even, then the maximum stable $2^{k-1}, \cdots, (2^k - 2)$ or $(2^k - 1)$-error linear complexity of s are all $2^n - (2^k - 1)(k > 0)$.

The following is an example to illustrate Corollary 3.2.2.

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 are all $2^n-(2^k-1)$.

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 are not decreased, so the original sequence possesses stable e-error linear complexity.

According to Lemma 2.1.2 in Section 2.1, 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 are all $2^n-(2^k-1)$.

By combining Corollary 3.2.1 and Corollary 3.2.2, we can achieve the following theorem.

Theorem 3.2.3 For $2^{l-1} \le k < 2^l$, there exists a 2^n-periodic binary sequence s with stable 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.

Niu *et al.* (2013, 2014) gave the following result.

Conjecture 3.2.1 Let $L_m(s)$ the m-error linear complexity of binary sequence with period 2^n. Then $L_m(s) \le 2^n-2m+1$.

Theorem 3.2.3 completely answers Conjecture 3.2.1. If $m=2^{l-1}$, then there exists a 2^n-periodic binary sequence s such that $L_m(s)=2^n-2^l+1=2^n-2m+1$. Otherwise, if $m=2^{l-1}+v$, where $v>0$, then $L_m(s)=2^n-2^l+1=2^n-2m+2v+1>2^n-2m+1$. In other words, Conjecture 3.2.1 is correct only when $m=2^{l-1}$, in other cases it is not correct.

It is reminded that the CELCS (critical error linear complexity spectrum) is studied by Lauder and Paterson (2003); Etzion *et al.* (2009). The CELCS of a sequence s consists of the ordered set of points $(k, L_k(s))$ satisfying $L_k(s) > L_{k'}(s)$, for $k' > k$; these are the points where a decrease occurs in the k-error linear complexity, and thus are called critical points. An efficient algorithm for computing the CELCS of a sequence is given by Lauder and Paterson (2003).

Let s be a binary sequence with period 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 will study binary sequences with several cubes. By Theorem 3.2.2, if s is a 2^n-periodic binary sequence, then it can be decomposed into several disjoint cubes. The following examples show that the cube decomposition of a sequence is not unique.

For example, $1 + x + x^3 + x^4 + x^7 + x^8$ can be decomposed into a 1-cube $1 + x$, whose linear complexity is $2^n - 1$, and a 2-cube $x^3 + x^4 + x^7 + x^8$, whose linear complexity is $2^n - (1 + 4)$.

It can also be decomposed into a 1-cube $x^3 + x^4$, whose linear complexity is $2^n - 1$, a 1-cube $x + x^7$, whose linear complexity is $2^n - 2$, and another 1-cube $1 + x^8$, whose linear complexity is $2^n - 8$.

It can also be decomposed into a 1-cube $x^7 + x^8$, whose linear complexity is $2^n - 1$, a 1-cube $x + x^3$, whose linear complexity is $2^n - 2$, and another 1-cube $1 + x^4$, whose linear complexity is $2^n - 4$.

It can also be decomposed into a 1-cube $1 + x^3$, whose linear complexity is $2^n - 1$, a 1-cube $x + x^7$, whose linear complexity $2^n - 2$, and another 1-cube $x^4 + x^8$, whose linear complexity is $2^n - 4$.

.....

In fact, we do not know how many possible ways for such decompositions. However, in order to achieve the maximal decrease of the linear complexity of the new sequence by superposing another sequence over the original one, a direct method is, if possible, that the linear complexity of the first cube is changed to the same as the linear complexity of the second cube.

As an illustrative example, noting that the linear complexity of $x^3 + x^4 + x^7 + x^8$ is $2^n - 5$, thus in order to achieve the maximum decrease of linear complexity, we superpose $x^{12} + x^{13}$ over $1 + x + x^3 + x^4 + x^7 + x^8$, so that the linear complexity of $1 + x + x^{12} + x^{13}$ is also $2^n - 5$. As a result, the linear complexity of $1 + x + x^3 + x^4 + x^7 + x^8 + x^{12} + x^{13}$ is reduced to $2^n - 6$, which can be decomposed into a 2-cube $x + x^3 + x^7 + x^{13}$, whose linear complexity is $2^n - 6$, and another 2-cube $1 + x^4 + x^8 + x^{12}$, whose linear complexity is $2^n - 12$.

To construct the sequence possessing high stable k-error linear complexity, both the first cube and the second cube should possess higher linear complexity. Specifically, it is easy to verify the following.

Theorem 3.2.4 Suppose that s is a binary sequence with period 2^n, the linear complexity of the largest cube of s is $L(s) = 2^n-(2^{i_1}+2^{i_2}+\cdots+2^{i_m})$, where $0 \leq i_1 < i_2 < \cdots < i_m < n$, and the linear complexity of the second largest cube of s is $2^n - (2^{j_1} + 2^{j_2} + \cdots + 2^{j_l})$, where $0 \leq j_1 < j_2 < \cdots < j_l < n$. If the largest cube of s is unique, then $2^m + 2^l$ is the minimum number k for which the second decrease occurs in the k-error linear complexity of s. Namely,

$$L(s) > L_{2^m}(s) > L_{2^m+2^l}(s).$$

For example, $1+x+x^3+x^4+x^7+x^8$ has a 1-cube $1+x$, whose linear complexity is 2^n-1. It also has 1-cube x^3+x^4 and x^7+x^8, all with linear complexity 2^n-1. So Theorem 3.2.4 can not be applied to this sequence. In fact, $L(s) > L_2(s) > L_4(s) > 0$.

3.3 Summary

A small number of element changes may lead to a sharp decline of linear complexity, so the concept of stable k-error linear complexity has been introduced in this chapter. 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 is operated,the **cube theory** has been proposed to study the k-error linear complexity. Further, a new approach to constructing the sequence with stable k-error linear complexity based on the cube theory has been derived. It has been proved that a binary sequence whose period is 2^n can be decomposed into several disjoint cubes. Based on the Games-Chan algorithm (Games and Chan, 1983) a **standard cube decomposition** of sequence $s^{(n)}$ has also been proposed.

In future, by using methods similar to that of the binary sequence, we may study a sequence with period p^n over F_p, where p is a prime number. The polynomial $1 - x^{p^n} = (1 - x)^{p^n}$ over F_p. Thus for a sequence with period p^n over F_p, its linear complexity is equal to the degree of factor $(1 - x)$ in $s^N(x)$.

Chapter 4

A Structural Approach for Determining the CELCS of 2^n-periodic Binary Sequences

In this chapter, we propose a structural approach to determining the CELCS (critical error linear complexity spectrum) (Lauder and Paterson, 2003; Etzion *et al.*, 2009) for the k-error linear complexity distribution of 2^n-periodic binary sequences. To explain the difference of Chapter 2 and this chapter, we give the following example.

Suppose that $s^{(n)}$ is a 2^n-periodic binary sequence. Let $N_k(L)$ be the number of 2^n-periodic binary sequences $s^{(n)}$ with linear complexity 2^n and the k-error linear complexity L. The complete counting function $N_1(L)$ is obtained by Meidl (2005). The complete counting function $N_3(L)$ is derived in Section 2.4 of Chapter 2. Partial counting function $N_5(L)$ is given in Section 2.6 of Chapter 2.

Let $N_{i,k}(L)$ be the number of 2^n-periodic binary sequences $s^{(n)}$ with linear complexity 2^n, the i-error linear complexity as the last descent point and the k-error linear complexity being L. Then we can have

$$N_5(L) = N_{1,5}(L) + N_{3,5}(L) + N_{5,5}(L) + \sum N_{i|i>5,5}(L)$$

In this chapter, we mainly focus on $N_{i,k}(L)$ **of 2^n-periodic binary sequences** $s^{(n)}$ with linear complexity 2^n or linear complexity less than 2^n. In contrast, Chapter 2 mainly focuses on $N_k(L)$ **of 2^n-periodic binary sequences** $s^{(n)}$ with linear complexity 2^n or linear complexity less than 2^n.

Another difference is that the proposed structural approach is based on **the Cube Theory** of Chapter 3.

Similar to Chapter 2, we will study the k-error linear complexity of 2^n-periodic binary sequences by using the sieve approach and the Games-Chan algorithm (Games and Chan,

1983). The structural approach is also based on the proposed framework in Chapter 2. Let $S = \{s|L(s) = c\}, E = \{e|W_H(e) = k\}, S + E = \{s + e|s \in S, e \in E\}$, where s is a sequence with linear complexity c and e is a sequence with $W_H(e) = k$. With the following sieve method, we aim to sieve sequences $s+e$ with $L_k(s+e) = c$ from $S+E$. For given linear complexity c, it remains to investigate two cases. One is that $s + u \in S + E$, but $L_k(s + u) < c$. This is equivalent to checking if there exists a sequence v such that $L(u+v) = c$. The other is the case that $s+u, t+v \in S+E$ and $L_k(s+u) = L_k(t+v) = c$ with $s \neq t$, $u \neq v$, but $s + u = t + v$. It is equivalent to checking if there exists a sequence v such that $L(u+v) = L(s+t) < c$ and if so, check the number of such sequence v, where $W_H(u) = W_H(v) = k$.

Finally in Section 4.4, first the k-error cube decomposition of 2^n-periodic binary sequences is developed based on **the Cube Theory** of Chapter 3. Based on the proposed k-error cube decomposition, and the famous inclusion-exclusion principle, we obtain the complete characterization of the ith descent point (critical point) of the k-error linear complexity for $i = 2, 3$, which are the extension of the work by Kurosawa *et al.* (2000). In fact, the proposed constructive approach has the potential to be used for constructing 2^n-periodic binary sequences with the given linear complexity and k-error linear complexity (or CELCS), which is a challenging problem to be deserved for further investigation in future.

The rest of this chapter is organized as follows. In Section 4.1, we mainly investigate 2^n-periodic binary sequences with given first descent point of 1-error linear complexity and second descent point of 3-error linear complexity. In Section 4.2, we study 2^n-periodic binary sequences with given first descent point of 2-error linear complexity and second descent point of 4-error linear complexity. In Section 4.3, 2^n-periodic binary sequences with given first descent point of 1-error linear complexity, second descent point of 3-error linear complexity and third descent point of 5-error linear complexity are discussed. Finally in Section 4.4, first the k-error cube decomposition of 2^n-periodic binary sequences is developed based on **the Cube Theory** of Chapter 3. Second we investigate the formulas to determine the second descent points and third descent points for the k-error linear complexity, respectively.

4.1 2^n-periodic binary sequences with given 3-error linear complexity as the second descent point

Suppose that $s^{(n)}$ is a 2^n-periodic binary sequence. We first investigate the relationship between the first descent point of the k-error linear complexity and the second descent point of the k-error linear complexity. Second, based on the first descent point and the second descent point, we obtain the complete counting functions of 2^n-periodic binary sequences with given first descent point of 1-error linear complexity and second descent point of 3-error linear complexity.

Theorem 4.1.1 Let $s^{(n)}$ be a 2^n-periodic binary sequence with linear complexity 2^n. Then $L_3(s^{(n)}) < L_1(s^{(n)})$ if and only if $L_1(s^{(n)}) = 2^n - (2^i + 2^j), 0 \leq i < j < n$.

Proof. $\Rightarrow$

By result from Kurosawa *et al.* (2000) we know that the minimum number k for which the k-error linear complexity of 2^n-periodic binary sequence with linear complexity $2^n-(2^i+2^j)$ is strictly less than $2^n - (2^i + 2^j)$ is $2^2 = 4$. Note that from the sequence with linear complexity $L_1(s^{(n)})$ to the sequence with linear complexity $L_3(s^{(n)})$, at most 4 elements have been changed. Thus, if $L_3(s^{(n)}) < L_1(s^{(n)})$, then $s^{(n)}$ is obtained by changing one element of a 2^n-periodic binary sequence with linear complexity $2^n-(2^i+2^j)$. So $L_1(s^{(n)}) = 2^n - (2^i + 2^j)$.

$\Leftarrow$

Suppose that $L_1(s^{(n)}) = 2^n - (2^i + 2^j)$. Similarly by result from Kurosawa *et al.* (2000) we know that it is possible to change 3 elements of $s^{(n)}$, so that the new sequence with linear omplexity less then $2^n - (2^i + 2^j)$. That is $L_3(s^{(n)}) < L_1(s^{(n)})$.

□

Next we investigate the distribution of $L_3(s^{(n)})$ in the following theorem.

Theorem 4.1.2 Let $s^{(n)}$ be a 2^n-periodic binary sequence with linear complexity 2^n. If $L_1(s^{(n)}) = 2^n-(2^i+2^j), 0 \leq i < j < n$, then $L_3(s^{(n)}) = 2^n-(2^{i_1}+2^{i_2}+\cdots+2^{i_m}) < 2^n-(2^i+2^j)$, where $0 \leq i_1 < i_2 < \cdots < i_m < n, m > 2$, or $L_3(s^{(n)}) = 2^n-(2^{i_1}+2^{i_2}) < 2^n-(2^i+2^j)$, where $i_1 \neq i, j$ and $i_2 \neq j$.

Proof. The following proof is based on the framework: $S+E=\{t+e|t\in S, e\in E\}$.

We only give the following example to illustrate the proof.

Let $s^{(4)}$ be a 2^4-periodic binary sequence with linear complexity 2^4. If $L_1(s^{(4)})=2^4-(2^0+2)$, then $L_3(s^{(4)})\neq 2^4-(2+2^3)$.

We will prove it by contradiction. Suppose that $L_3(s^{(4)})=2^4-(2+2^3)$. Let $S=\{t|L(t)=2^4-(2+2^3)\}, E=\{e|W_H(e)=3\}, S+E=\{t+e|t\in S, e\in E\}$, where t is a sequence with linear complexity $2^4-(2+2^3)$ and e is a sequence with $W_H(e)=3$. With the sieve method, we aim to sieve sequences $t+e$ with $L_3(t+e)=2^4-(2+2^3)$ from $S+E$.

We now investigate the case that $t+u\in S+E$, but $L_3(t+u)<2^4-(2+2^3)$. This is equivalent to checking if there exists a sequence $v\in E$ such that $L(u+v)=2^4-(2+2^3)$.

For any $u\in E$ such that $L_1(t+u)=2^4-(1+2)$. Such as $u=\{1110\ 0000\ 0000\ 0000\}$. There exists a sequence $v\in E$ such that $L(u+v)=2^4-(2+2^3)$. So $L_3(t+u)<2^4-(2+2^3)$. Here $v=\{0100\ 0000\ 1010\ 0000\}$.

This completes the proof. □

We next derive the counting formula of binary sequences with both the given 1-error linear complexity and the given 3-error linear complexity.

Theorem 4.1.3 Let $s^{(n)}$ be a 2^n-periodic binary sequence with linear complexity 2^n.

1) If $L_1(s^{(n)})=2^n-(2^i+2^j), 0\leq i<j<n$, and $L_3(s^{(n)})=2^n-(2^{i_1}+2^{i_2}+\cdots+2^{i_m})<2^n-(2^i+2^j)$, where $0\leq i_1<i_2<\cdots<i_m<n, m>2$ or $L_3(s^{(n)})=2^n-(2^{i_1}+2^{i_2})<2^n-(2^i+2^j)$, where $i_1\neq i,j$ and $i_2\neq j$. Then the number of 2^n-periodic binary sequences $s^{(n)}$ can be given by

$$2^{3n-j-i-3}\times 2^{L-1}/(2^{\epsilon+j-i_0}\times 8^{n-i_m-1})$$

where $i_0\leq j$ is the minimum number for which $2^n-(2^{i_0}+2^j)<2^n-(2^{i_1}+2^{i_2}+\cdots+2^{i_m})$ with a default choice $i_0=j$. Further, if $j=i_m$ or $2^n-(2^j+2^{i_m})>L_3(s^{(n)})$ then $\epsilon=0$, if $j<i_m$ and only $2^n-(2^j+2^{i_m})<L_3(s^{(n)})$ then $\epsilon=1$, if $2^n-(2^i+2^{i_m})<L_3(s^{(n)})$ then $\epsilon=2$, where $i_m=i_2$ for $L=2^n-(2^{i_1}+2^{i_2})$.

2) If $L_3(s^{(n)})=0$, then the number of 2^n-periodic binary sequences $s^{(n)}$ can be given by $2^{3n-j-i-3}$.

Proof. 1) Let $S = \{t|L(t) = L\}, E = \{e|W_H(e) = 3\}, S + E = \{t + e|t \in S, e \in E\}$, where t is a sequence with linear complexity $L = 2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m})$ and e is a sequence with $W_H(e) = 3$ and $L_1(e) = 2^n - (2^i + 2^j)$. With the sieve method, we aim to sieve sequences $t + e$ with $L_3(t + e) = L$ from $S + E$.

By Lemma 2.1.6 in Section 2.1, we know that the number of 2^n-periodic binary sequences t with $L(t) = L$ is 2^{L-1}. Now we will obtain the number of sequences e with $W_H(e) = 3$ and $L_1(e) = 2^n - (2^i + 2^j)$.

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 3.1.1 in Section 3.1, the number of these $s^{(j)}$ can be given by $(2^2)^{j-i-1} \times 2^i = 2^{2j-i-2}$.

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

$\{1010\ 0000\}$, $\{1000\ 0010\}$, $\{0010\ 1000\}$, $\{0000\ 1010\}$

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}.

As $u \in E$ such that $L_1(u) = 2^n - (2^i + 2^j)$. So the number of these u can be given by

$$2^2 \times (2^3)^{n-j-1} \times 2^{2j-i-2} = 2^{3n-j-i-3}.$$

We now investigate the case that $s + u, t + v \in S + E$ and $L_3(s + u) = L_3(t + v) = L$ with $s \neq t$, $u \neq v$, but $s + u = t + v$. It is equivalent to checking if there exists a sequence v such that $L(u + v) = L(s + t) < L$ and if so, check the number of such sequence v, where $W_H(u) = W_H(v) = 3$. We need to consider the following two cases.

The first case is related to the minimum $i_0 \leq j$ such that $2^n - (2^{i_0} + 2^j) < L = 2^n - (2^{i_1} +$

$2^{i_2} + \cdots + 2^{i_m}$). For any $u \in E$, it is easy to show that there exist $2^{j-i_0} - 1$ sequences v, such that $L(u+v) < L$.

(The following example is given to illustrate the above case. Suppose that $n = 5, i = 0, j = 4, i_0 = 2$, $i_1 = 0, i_2 = 1, i_3 = 4$. So $L = 2^n - (2^{i_1} + 2^{i_2} + 2^{i_3}) = 13$.

If $u^{(5)} = \{1100\ 0000\ 0000\ 0000\ 1000\ 0000\ 0000\ 0000\}$. Then

$v_1^{(5)} = \{0100\ 0000\ 1000\ 0000\ 0000\ 0000\ 1000\ 0000\}$,

$v_2^{(5)} = \{0100\ 1000\ 0000\ 0000\ 0000\ 1000\ 0000\ 0000\}$,

$v_3^{(5)} = \{0100\ 0000\ 0000\ 1000\ 0000\ 0000\ 0000\ 1000\}$.

Thus $L(u^{(5)} + v_1^{(5)}) = 2^5 - (2^3 + 2^4)$, $L(u^{(5)} + v_2^{(5)}) = L(u^{(5)} + v_3^{(5)}) = 2^5 - (2^2 + 2^4)$.)

The second case is related to $i_m < w < n$. For $i_m < w < n$, there exist $7 \times 8^{w-i_m-1}$ sequences v, such that $L(u+v) = 2^n - (2^i + 2^w) < L$ or $L(u+v) = 2^n - (2^j + 2^w) < L$ or $L(u+v) = 2^n - 2^w < L$.

Note that for any sequence v with 3 nonzero elements, if we double the period of sequence v, then 2^3 new sequences will be generated. Therefore there exist

$$7 + 7 \times 8 + \cdots + 7 \times 8^{n-i_m-2} = 8^{n-i_m-1} - 1$$

sequences v, such that $L(u+v) < L$.

(The following example is given to illustrate the above case. Suppose that $n = 5, i = 0, j = 1, i_1 = 1, i_2 = 2, i_3 = 3$,

$u^{(5)} = \{1110\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\}$. Then

$v_1^{(5)} = \{0100\ 0000\ 0000\ 0000\ 1010\ 0000\ 0000\ 0000\}$,

$v_2^{(5)} = \{1000\ 0000\ 0000\ 0000\ 0110\ 0000\ 0000\ 0000\}$,

$v_3^{(5)} = \{0010\ 0000\ 0000\ 0000\ 1100\ 0000\ 0000\ 0000\}$,

$v_4^{(5)} = \{0110\ 0000\ 0000\ 0000\ 1000\ 0000\ 0000\ 0000\}$,

$v_5^{(5)} = \{1010\ 0000\ 0000\ 0000\ 0100\ 0000\ 0000\ 0000\}$,

$v_6^{(5)} = \{1100\ 0000\ 0000\ 0000\ 0010\ 0000\ 0000\ 0000\}$,

$v_7^{(5)} = \{0000\ 0000\ 0000\ 0000\ 1110\ 0000\ 0000\ 0000\}$.

Thus $L(u^{(5)} + v_1^{(5)}) = 2^5 - (2 + 2^4)$, $L(u^{(5)} + v_2^{(5)}) = L(u^{(5)} + v_3^{(5)}) = 2^5 - (1 + 2^4)$, $L(u^{(5)} + v_4^{(5)}) = L(u^{(5)} + v_5^{(5)}) = L(u^{(5)} + v_6^{(5)}) = L(u^{(5)} + v_7^{(5)}) = 2^5 - 2^4$.)

If $j < i_m$ and only $2^n - (2^j + 2^{i_m}) < L$ then the number of v will be increased by 8^{n-i_m-1}.

If $2^n - (2^i + 2^{i_m}) < L$ then the number of v will be increased by $3 \times 8^{n-i_m-1}$.

It follows that the number of 2^n-periodic binary sequences $s^{(n)}$ with $L_1(s^{(n)}) = 2^n - (2^i + 2^j)$ and $L_3(s^{(n)}) = L$ can be given by

$$2^{3n-j-i-3} \times 2^{L-1}/(2^{\epsilon+j-i_0} \times 8^{n-i_m-1})$$

where if $j = i_m$ or $2^n - (2^j + 2^{i_m}) > L$ then $\epsilon = 0$, if only $2^n - (2^j + 2^{i_m}) < L$ then $\epsilon = 1$, if $2^n - (2^i + 2^{i_m}) < L$ then $\epsilon = 2$.

If $j > i_0$, then $2^n - (2^{i_0} + 2^j) < 2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m}) < 2^n - (2^i + 2^j)$, so $j = i_m$. If $\epsilon > 0$, then $j < i_m$. Therefore, $j - i_0$ and ϵ can not be positive at the same time.

We can use almost the same method to deal with the case of $L_3(s^{(n)}) = 2^n - (2^{i_1} + 2^{i_2})$ but without the situation of $j = i_2$.

2) This is an obvious case. □

To further illustrate Theorem 4.1.3, we give the following two examples, which are verified by computer program as well.

Example 4.1.1 Suppose that $n = 4, i = 1, j = 3, i_0 = 2, i_1 = 0, i_2 = 1, i_3 = 3$. Note that $L = 2^n - (2^{i_1} + 2^{i_2} + 2^{i_3}) = 2^4 - (1 + 2 + 8) = 5$, so $2^n - (2^{i_0} + 2^j) = 2^4 - (4 + 8) < L$. As $j = i_3$, so $\epsilon = 0$. The number of 2^4-periodic binary sequences $s^{(4)}$ with $L_1(s^{(4)}) = 6$ and $L_3(s^{(4)}) = 5$ can be given by

$$2^{3\times n-3-1-3} \times 2^{5-1}/(2^1 \times 8^{4-3-1}) = 2^8.$$

Example 4.1.2 Suppose that $n = 4, i = 1, j = 2, i_1 = 0, i_2 = 3$. Note that $L = 2^n - (2^{i_1} +$

$2^{i_2}) = 2^4 - (1+8) = 7$. As $j < i_2$, $2^n - (2^j + 2^{i_2}) = 4 < L$ and $2^n - (2^i + 2^{i_2}) = 6 < L$, so $\epsilon = 2$. The number of 2^4-periodic binary sequences $s^{(4)}$ with $L_1(s^{(4)}) = 10$ and $L_3(s^{(4)}) = 7$ can be given by

$$2^{3\times n-2-1-3} \times 2^{7-1}/(2^2 \times 8^{4-3-1}) = 2^{10}.$$

4.2 2^n-periodic binary sequences with the given 4-error linear complexity as second descent point

Next we derive the counting formula of 2^n-periodic binary sequences with both the given 2-error linear complexity as first descent point and the 4-error linear complexity as second descent point. To this end, we will use *the Cube Theory* of of Chapter 3.

It is known by result from Kurosawa *et al.* (2000) that for a 2^n-periodic binary sequence with linear complexity $2^n - (2^i + 2^j), 0 \leq i < j < n$, the 4-error linear complexity is the first descent point. In contrast, with the cube theory we will characterize 2^n-periodic binary sequences with the 4-error linear complexity as second descent point.

Next we use a sequence 1101 1001 1000 0000 to illustrate the standard cube decomposition (in Section 3.2) process and its critical points. 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 $Left \bigoplus Right$. Then the cube $1 + x^8$ is removed.

Recursively, as $Left \neq Right$, then we consider $Left \bigoplus Right$. This time the cube $x^3 + x^7$ is removed. Only cube $x + x^4$ is retained. 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 2.1.2 in Section 2.1, 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 (see definition in section 3.2) of $1 + x + x^3 + x^4 + x^7 + x^8$ are $(0, 2^n - 1) = (0, 15)$,$(2, 2^n - (2 + 4)) = (2, 10)$,$(4, 2^n - (8 + 4 + 1)) = (4, 3)$,$(6, 0)$. Here $(4, 3)$ corresponds polynomial $1 + x^3 + x^4 + x^7 + x^8 + x^{11} + x^{12} + x^{15}$.

Theorem 4.2.1 Let $s^{(n)}$ be a 2^n-periodic binary sequence with linear complexity less than 2^n. Then

i). Suppose that c_1 and c_2 are in the standard cube decomposition of sequence $s^{(n)}$ and $L(s^{(n)}) = L(c_1)$. If $L_4(s^{(n)}) < L_2(s^{(n)}) < L(s^{(n)})$, then c_1 and c_2 are two 1-cubes or c_1 is a 1-cube and c_2 is a 2-cube;

ii). $L_4(s^{(n)}) < L_2(s^{(n)}) < L(s^{(n)})$ if and only if $L_2(s^{(n)}) = 2^n - (2^i + 2^j), 0 \leq i < j < n$, but $L_2(s^{(n)}) \neq 2^n - (1 + 2)$;

iii). If $L(s^{(n)}) = 2^n - 2^{i_0}$, then $i_0 < i$ or $i < i_0 < j$, where i and j are defined in ii).

Proof. i). Suppose that $s^{(n)}$ is a 2^n-periodic binary sequence with linear complexity $2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m})$. By Kurosawa *et al.* (2000) we know that the minimum number k for which the k-error linear complexity of 2^n-periodic binary sequence $s^{(n)}$ is strictly less than the linear complexity of $s^{(n)}$ is 2^m. So the proof is obvious.

ii). Based on i), here we only need to prove that $L_2(s^{(n)}) \neq 2^n - (1 + 2)$.

In the case that c_1 and c_2 are two 1-cubes. As $L(s^{(n)}) \neq 2^n - (1 + 2)$, there exist two nonzero elements with distance $d > 2$ in c_1 and c_2. Suppose that $L_2(s^{(n)}) = 2^n - (2^i + 2^j)$. Then $2^j \geq d > 2$. It follows that $L_2(s^{(n)}) \neq 2^n - (1 + 2)$.

In the case that c_1 is a 1-cube and c_2 is a 2-cube. If $L(c_2) = 2^n - (1+2)$, then $L(c_1) = 2^n - 1$ or $2^n - 2$. There exist two nonzero elements with distance $d > 2$ in c_1 and c_2. Suppose that $L_2(s^{(n)}) = 2^n - (2^i + 2^j)$. Then $2^j \geq d > 2$. It follows that $L_2(s^{(n)}) \neq 2^n - (1 + 2)$.

iii). Based on i) and ii), it is easy to prove iii). □

Next we investigate the distribution of $L_4(s^{(n)})$.

Theorem 4.2.2 Let $s^{(n)}$ be a 2^n-periodic binary sequence with linear complexity $L(s^{(n)}) = 2^n - 2^{i_0}$. If $L_4(s^{(n)}) < L_2(s^{(n)}) < L(s^{(n)})$ and $L_2(s^{(n)}) = 2^n - (2^i + 2^j), 0 \leq i < j < n$, then $L_4(s^{(n)}) = 2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m}) < 2^n - (2^i + 2^j)$, where $0 \leq i_1 < i_2 < \cdots < i_m < n, m > 3$, or $L_4(s^{(n)}) = 2^n - (2^{i_1} + 2^{i_2} + 2^{i_3})$, where $\{i_1, i_2, i_3\} \neq \{i, j, i_0\}$, $\{i_1, i_2, i_3\} \neq \{0, 1, 2\}$, or $L_4(s^{(n)}) = 2^n - (2^{i_1} + 2^{i_2}) < 2^n - (2^i + 2^j)$, where $i_2 \neq j$, $i_1 \neq i, j, i_0$.

Proof. The following proof is based on the framework: $S + E = \{t + e | t \in S, e \in E\}$.

In the case that $L_4(s^{(n)}) = 2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m}) < 2^n - (2^i + 2^j)$, the proof is obvious.

In the case that $L_4(s^{(n)}) = 2^n - (2^{i_1} + 2^{i_2}) < 2^n - (2^i + 2^j)$. We only give the following example to illustrate the proof.

Let $s^{(4)}$ be a 2^4-periodic binary sequence with linear complexity less than 2^4. If $L(s^{(4)}) = 2^4 - 2$ and $L_2(s^{(4)}) = 2^4 - (1 + 2^2)$, then $L_4(s^{(4)}) \neq 2^4 - (2 + 2^2)$.

Suppose that $L_4(s^{(4)}) = 2^4 - (2 + 2^2)$. Let $S = \{t | L(t) = 2^4 - (2 + 2^2)\}, E = \{e | W_H(e) = 4\}, S + E = \{t + e | t \in S, e \in E\}$, where t is a sequence with linear complexity $2^4 - (2 + 2^2)$ and e is a sequence with $W_H(e) = 4$. With the sieve method, we aim to sieve sequences $t + e$ with $L_4(t + e) = 2^4 - (2 + 2^2)$ from $S + E$.

We now investigate the case that $s + u \in S + E$, but $L_4(t + u) < 2^4 - (2 + 2^2)$. This is equivalent to checking if there exists a sequence $v \in E$ such that $L(u + v) = 2^4 - (2 + 2^2)$.

For any $u \in E$ such that $L_2(t + u) = 2^4 - (1 + 4)$. Such as $u = \{1100\ 0110\ 0000\ 0000\}$. There exists a sequence $v \in E$ such that $L(u+v) = 2^4-(2+2^2)$. So $L_4(t+u) < 2^4-(2+2^2)$. Here $v = \{1001\ 0011\ 0000\ 0000\}$ such that $L_2(t + v) = 2^4 - (1 + 4)$. Therefore $i_2 \neq j$.

Let $L(t) = 2^4-(1+2^3)$. There exists a sequence $v \in E$ such that $L(u+v) = 2^4-(1+2^3)$. So $L_4(t+u) < 2^4-(1+2^3)$. Here $v = \{0000\ 0110\ 1100\ 0000\}$ such that $L_2(t+v) = 2^4-(1+2^2)$. Therefore $i_1 \neq i$.

Let $L(t) = 2^4-(2^2+2^3)$. There exists a sequence $v \in E$ such that $L(u+v) = 2^4-(2^2+2^3)$. So $L_4(t + u) < 2^4 - (2^2 + 2^3)$. Here $v = \{1000\ 0010\ 0100\ 0100\}$ such that $L_2(t + v) = 2^4 - (1 + 2^2)$. Therefore $i_1 \neq j$.

Let $L(t) = 2^4-(2+2^3)$. There exists a sequence $v \in E$ such that $L(u+v) = 2^4-(2+2^3)$. So $L_4(t+u) < 2^4-(2+2^3)$. Here $v = \{0100\ 0100\ 1000\ 0010\}$ such that $L_2(t+v) = 2^4-(1+2^2)$. Therefore $i_1 \neq i_0$.

In the case that $L_4(s^{(n)}) = 2^n - (2^{i_1} + 2^{i_2} + 2^{i_3})$. Note that c_1 is a 1-cube and c_2 is a 2-cube, $L(c_2) = L_2(s^{(n)}) = 2^n - (2^i + 2^j)$. We also use the following example to illustrate the proof.

Suppose that $n = 4, i = 0, j = 3, i_0 = 2$, $u^{(4)} = \{0100\ 1000\ 1100\ 0000\}$.

Then there exists $v^{(4)} = \{1000\ 0100\ 0000\ 1100\}$, such that $L(u^{(4)}+v^{(4)}) = 2^4-(1+2^2+2^3)$.

Therefore $L_4(s^{(n)}) \neq 2^n - (2^{i_1} + 2^{i_2} + 2^{i_3})$, where $\{i_1, i_2, i_3\} = \{i, i_0, j\}$.

Now we consider the case that $L_4(s^{(n)}) = 2^n - (2^0 + 2^1 + 2^2)$. As $L_4(s^{(n)}) < 2^n - (2^i + 2^j) < 2^n - 2^{i_0}$, so $2^{i_0} < 2^i + 2^j < 2^0 + 2^1 + 2^2$. Suppose that $L(t) = 2^n - (2^0 + 2^1 + 2^2)$. For any $u \in E$ such that $L_2(t+u) = 2^n - (2^i + 2^j)$. It is easy to prove that $L_4(t+u) < 2^n - (2^0 + 2^1 + 2^2)$. We just use the following example to illustrate the proof.

Suppose that $n = 4, i = 0, j = 2, i_0 = 1$, $u^{(4)} = \{0110\ 1100\ 0000\ 0000\}$ and $t^{(4)} = \{1111\ 1111\ 0000\ 0000\}$, then $t^{(4)} + u^{(4)} = \{1001\ 0011\ 0000\ 0000\}$. So, $L_4(t^{(4)} + u^{(4)}) = 0$.

If $t^{(4)} = \{1111\ 0011\ 0000\ 1100\}$, then $L_4(t^{(4)} + u^{(4)}) = 2^4 - (2^0 + 2^3)$.

This completes the proof. □

We next derive the counting formula of binary sequences with both the given 2-error linear complexity and the given 4-error linear complexity.

Theorem 4.2.3 Let $s^{(n)}$ be a 2^n-periodic binary sequence with linear complexity $L(s^{(n)}) = 2^n - 2^{i_0}$.

1) If $L_4(s^{(n)}) < L_2(s^{(n)}) < L(s^{(n)})$ and $L_2(s^{(n)}) = 2^n - (2^i + 2^j), 0 \leq i < j < n$, and $L_4(s^{(n)}) = 2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m}) < 2^n - (2^i + 2^j)$, where $0 \leq i_1 < i_2 < \cdots < i_m < n, m > 3$ or $L_4(s^{(n)}) = 2^n - (2^{i_1} + 2^{i_2} + 2^{i_3})$, where $\{i_1, i_2, i_3\} \neq \{i, j, i_0\}$, $\{i_1, i_2, i_3\} \neq \{0, 1, 2\}$, or $L_4(s^{(n)}) = 2^n - (2^{i_1} + 2^{i_2}) < 2^n - (2^i + 2^j)$, where $i_2 \neq j$, $i_1 \neq i, j, i_0$. Then the number of 2^n-periodic binary sequences $s^{(n)}$ can be given by

$$(2^{4n-j-i-4-i_0}/\gamma) \times 2^{L-1}/(2^{\delta+\epsilon} \times 16^{n-i_m-1})$$

where if $i_0 > i$ then $\gamma = 2$ else $\gamma = 1$; if $2^n - (2^i + 2^{i_0} + 2^j) > L$ then $\delta = 0$, if only $2^n - (2^i + 2^{i_0} + 2^j) < L$ then $\delta = 1$, if $2^n - (2^{i_0} + 2^j) < L$ then $\delta = 2$. Further, if $j = i_m$ or $2^n - (2^j + 2^{i_m}) > L$ then $\epsilon = 0$, if $j < i_m$ and only $2^n - (2^j + 2^{i_m}) < L$ then $\epsilon = 1$, if $2^n - (2^i + 2^{i_m}) < L$ and $2^n - (2^{i_0} + 2^{i_m}) > L$ then $\epsilon = 2$, if $2^n - (2^i + 2^{i_m}) > L$ and $2^n - (2^{i_0} + 2^{i_m}) < L$ then $\epsilon = 2$, if $2^n - (2^i + 2^{i_m}) < L$ and $2^n - (2^{i_0} + 2^{i_m}) < L$ then $\epsilon = 3$, where $i_m = i_3$ for $L = 2^n - (2^{i_1} + 2^{i_2} + 2^{i_3})$ and $i_m = i_2$ for $L = 2^n - (2^{i_1} + 2^{i_2})$.

2) If $L_4(s^{(n)}) = 0$, then the number of 2^n-periodic binary sequences $s^{(n)}$ can be given by $2^{4n-j-i-4-i_0}/\gamma$, where if $i_0 > i$ then $\gamma = 2$ else $\gamma = 1$.

Proof. 1) Let $S = \{t | L(t) = L\}, E = \{e | W_H(e) = 4\}, S + E = \{t + e | t \in S, e \in E\}$, where t is a sequence with linear complexity $L = 2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m}), m > 2$ and e is

sequence with $W_H(e) = 4$ and $L_2(e) = 2^n - (2^i + 2^j)$. With the sieve method, we aim to sieve sequences $t + e$ with $L_4(t + e) = L$ from $S + E$.

By Lemma 2.1.6 in Section 2.1, we know that the number of 2^n-periodic binary sequences t with $L(t) = L$ is 2^{L-1}. Now we will compute the number of sequences e with $W_H(e) = 4$ and $L_2(e) = 2^n - (2^i + 2^j)$.

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 3.1.1 in Section 3.1, 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}.

As $u \in E$ such that $L_2(u) = 2^n - (2^i + 2^j)$. So the number of these u can be given by

$$2^2 \times \frac{2^{j+1}}{2^{i_0+1} \times \gamma} \times (2^4)^{n-j-1} \times 2^{2j-i-2} = 2^{4n-j-i-4-i_0}/\gamma$$

where if $i_0 > i$ then $\gamma = 2$ else $\gamma = 1$.

(The following example is given to illustrate the case of $i_0 > i$. Suppose that $n = 4, i = 0, j = 3, i_0 = 2$, $u^{(4)} = \{0100\ 0000\ 1100\ 1000\}$.

Then one obtains $v_1^{(4)} = \{1100\ 0000\ 1100\ 0000\}$, or $v_2^{(4)} = \{0100\ 1000\ 0100\ 1000\}$, where $L_2(v_1^{(4)}) = L_2(v_2^{(4)}) = 2^4 - (1 + 2^3)$.)

We now investigate the case that $s + u, t + v \in S + E$ and $L_4(s + u) = L_4(t + v) = L$ with $s \neq t$, $u \neq v$, but $s + u = t + v$. It is equivalent to checking if there exists a sequence v such that $L(u + v) = L(s + t) < L$ and if so, check the number of such sequence v, where $W_H(u) = W_H(v) = 4$. We need to consider the following two cases.

The first case is related to i_0. For any $u \in E$, there exists one sequence v, such that

$L(u+v) = 2^n - (2^i + 2^{i_0} + 2^j) < L$, and there exist two sequences v, such that $L(u+v) = 2^n - (2^{i_0} + 2^j) < L$.

(The following example is given to illustrate the above case. Suppose that $n = 4, i = 1, j = 3, i_0 = 2$, $u^{(4)} = \{1000\ 0010\ 1010\ 0000\}$. Then

$v_1^{(4)} = \{0010\ 1000\ 0000\ 1010\}$,

$v_2^{(4)} = \{0000\ 1010\ 0010\ 1000\}$,

$v_3^{(4)} = \{1010\ 0000\ 1000\ 0010\}$.

Thus $L(u^{(4)} + v_1^{(4)}) = 2^4 - (2 + 2^2 + 2^3)$, $L(u^{(4)} + v_2^{(4)}) = L(u^{(4)} + v_3^{(4)}) = 2^4 - (2^2 + 2^3)$.)

The second case is related to $i_m < w < n$. For $i_m < w < n$, there exist $15 \times 16^{w-i_m-1}$ sequences v, such that $L(u+v) = 2^n - (2^i + 2^w) < L$ or $L(u+v) = 2^n - (2^j + 2^w) < L$ or $L(u+v) = 2^n - (2^{i_0} + 2^w) < L$ or $L(u+v) = 2^n - 2^w < L$.

Note that for any sequence v with 4 nonzero elements, if we double the period of sequence v, then 2^4 new sequences will be generated. Therefore there exist

$$15 + 15 \times 16 + \cdots + 15 \times 16^{n-i_m-2} = 16^{n-i_m-1} - 1$$

sequences v, such that $L(u+v) < L$.

(The following example is given to illustrate the above case. Suppose that $n = 5, i = 0, j = 2, i_0 = 1, i_1 = 1, i_2 = 2, i_3 = 3, w = 4$,

$u^{(5)} = \{1001\ 1100\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\}$. Then

$v_1^{(5)} = \{0001\ 0100\ 0000\ 0000\ 1000\ 1000\ 0000\ 0000\}$.

Thus $L(u^{(5)} + v_1^{(5)}) = 2^5 - (2^2 + 2^4)$.

$v_2^{(5)} = \{1000\ 1000\ 0000\ 0000\ 0001\ 0100\ 0000\ 0000\}$,

$v_3^{(5)} = \{0000\ 0000\ 0000\ 0000\ 1001\ 1100\ 0000\ 0000\}$.

Thus $L(u^{(5)} + v_2^{(5)}) = L(u^{(5)} + v_3^{(5)}) = 2^5 - (2 + 2^4)$.

$v_4^{(5)} = \{1001\ 0000\ 0000\ 0000\ 0000\ 1100\ 0000\ 0000\}$,

$v_5^{(5)} = \{0000\ 1100\ 0000\ 0000\ 1001\ 0000\ 0000\ 0000\}$,

$v_6^{(5)} = \{0001\ 1000\ 0000\ 0000\ 1000\ 0100\ 0000\ 0000\}$,

$v_7^{(5)} = \{1000\ 0100\ 0000\ 0000\ 0001\ 1000\ 0000\ 0000\}$.

Thus $L(u^{(5)} + v_4^{(5)}) = L(u^{(5)} + v_5^{(5)}) = L(u^{(5)} + v_6^{(5)}) = L(u^{(5)} + v_7^{(5)}) = 2^5 - (1 + 2^4)$.

.....

$v_{15}^{(5)} = \{1000\ 0000\ 0000\ 0000\ 0001\ 1100\ 0000\ 0000\}$.

Thus $L(u^{(5)} + v_{15}^{(5)}) = 2^5 - 2^4$.)

On the other hand, if $j < i_m$ and only $2^n - (2^j + 2^{i_m}) < L$ then the number of v will be increased by 16^{n-i_m-1}.

If $2^n - (2^i + 2^{i_m}) < L$ and $2^n - (2^{i_0} + 2^{i_m}) > L$ then the number of v will be increased by $3 \times 16^{n-i_m-1}$.

If $2^n - (2^i + 2^{i_m}) > L$ and $2^n - (2^{i_0} + 2^{i_m}) < L$ then the number of v will be increased by $3 \times 16^{n-i_m-1}$.

If $2^n - (2^i + 2^{i_m}) < L$ and $2^n - (2^{i_0} + 2^{i_m}) < L$ then the number of v will be increased by $7 \times 16^{n-i_m-1}$.

It follows that the number of 2^n-periodic binary sequences $s^{(n)}$ with $L(s^{(n)}) = 2^n - 2^{i_0}$, $L_2(s^{(n)}) = 2^n - (2^i + 2^j)$ and $L_4(s^{(n)}) = L$ can be given by

$$(2^{4n-j-i-4-i_0}/\gamma) \times 2^{L-1}/(2^\delta \times 2^\epsilon \times 16^{n-i_m-1})$$

where if $2^n - (2^i + 2^{i_0} + 2^j) > L$ then $\delta = 0$, if only $2^n - (2^i + 2^{i_0} + 2^j) < L$ then $\delta = 1$, if $2^n - (2^{i_0} + 2^j) < L$ then $\delta = 2$; if $j = i_m$ or $2^n - (2^j + 2^{i_m}) > L$ then $\epsilon = 0$, if $j < i_m$ and only $2^n - (2^j + 2^{i_m}) < L$ then $\epsilon = 1$, if $2^n - (2^i + 2^{i_m}) < L$ and $2^n - (2^{i_0} + 2^{i_m}) > L$ then $\epsilon = 2$, if $2^n - (2^i + 2^{i_m}) > L$ and $2^n - (2^{i_0} + 2^{i_m}) < L$ then $\epsilon = 2$, if $2^n - (2^i + 2^{i_m}) < L$ and $2^n - (2^{i_0} + 2^{i_m}) < L$ then $\epsilon = 3$.

If $\delta > 0$, then $2^n - (2^i + 2^{i_0} + 2^j) < 2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m}) < 2^n - (2^i + 2^j)$, so $j = i_m$.

If $\epsilon > 0$, then $j < i_m$. Therefore, δ and ϵ can not be positive at the same time.

We can use almost the same method to deal with the case of $L_4(s^{(n)}) = 2^n - (2^{i_1} + 2^{i_2})$ but without the constraint of $j = i_2$.

2) This is an obvious case. □

To further illustrate Theorem 4.2.3, we give the following two examples, which are verified by computer program as well.

Example 4.2.1 Suppose that $n = 4, i = 1, j = 3, i_0 = 2, i_1 = 0, i_2 = 1, i_3 = 3$. Note that $i_0 > i$, so $\gamma = 2$. As $L = 2^n - (2^{i_1} + 2^{i_2} + 2^{i_3}) = 2^4 - (1 + 2 + 8) = 5$, so $2^n - (2^i + 2^{i_0} + 2^j) = 2^4 - (2 + 4 + 8) < L$ and $2^n - (2^{i_0} + 2^j) = 2^4 - (4 + 8) < L$. Thus $\delta = 2$. As $j = i_3$, so $\epsilon = 0$. The number of 2^4-periodic binary sequences $s^{(4)}$ with $L(s^{(4)}) = 12$, $L_2(s^{(4)}) = 6$ and $L_4(s^{(4)}) = 5$ can be given by

$$(2^{4\times n-3-1-4-2}/2) \times 2^{5-1}/(2^2 \times 16^{4-3-1}) = 2^7.$$

Example 4.2.2 Suppose that $n = 5, i = 2, j = 3, i_0 = 1, i_1 = 0, i_2 = 4$. Note that $i_0 < i$, so $\gamma = 1$. As $L = 2^n - (2^{i_1} + 2^{i_2}) = 2^5 - (1+16) = 15$, so $2^n - (2^i + 2^{i_0} + 2^j) = 2^5 - (4+2+8) > L$. Thus $\delta = 0$. As $j < i_2$ and $2^n - (2^i + 2^{i_2}) = 12 < L$ and $2^n - (2^{i_0} + 2^{i_2}) = 14 < L$ so $\epsilon = 3$. The number of 2^5-periodic binary sequences $s^{(5)}$ with $L(s^{(5)}) = 30$, $L_2(s^{(5)}) = 20$ and $L_4(s^{(5)}) = 15$ can be given by

$$2^{4\times n-3-2-4-1} \times 2^{15-1}/(2^3 \times 16^{5-4-1}) = 2^{21}.$$

4.3 2^n-periodic binary sequences with the given 5-error linear complexity as third descent point

Suppose that $s^{(n)}$ is a 2^n-periodic binary sequence. We first investigate the relationship among the first descent point, second descent point and third descent point of the k-error linear complexity. Second, based on the first descent point, second descent point and third descent point, we obtain the complete counting functions of 2^n-periodic binary sequences with the given 1-error, 3-error and 5-error linear complexity as the first, second and third descent points, respectively (Zhou *et al.*, 2015a).

Theorem 4.3.1 Let $s^{(n)}$ be a 2^n-periodic binary sequence with linear complexity 2^n. Then

i). Suppose that c_1, c_2 and c_3 are in the standard cube decomposition of sequence $s^{(n)}$. $L_5(s^{(n)}) < L_3(s^{(n)}) < L_1(s^{(n)})$ if and only if c_1 is a 0-cube (only one nonzero element), c_2 and c_3 are two 1-cubes or c_1 is a 0-cube and c_2 is a 2-cube;

ii). $L_5(s^{(n)}) < L_3(s^{(n)}) < L_1(s^{(n)})$ if and only if $L_1(s^{(n)}) = 2^n - (2^i + 2^j), 0 \leq i < j < n$, $L_3(s^{(n)}) = 2^n - (2^p + 2^q), 0 \leq p < q < n, j < q, p \neq i, j$, or $L_3(s^{(n)}) = 2^n - (2^i + 2^j + 2^r), 0 \leq r < n, r \neq i, j$.

Proof. Based on the cube theory, sequence $s^{(n)}$ has a standard cube decomposition. As $L(s^{(n)}) = 2^n$, it is obvious that c_1 is a 0-cube.

First, suppose that c_2 and c_3 are two 1-cubes. Then $L_1(s^{(n)}) = 2^n - (2^i + 2^j)$, where $0 \leq i < j < n, L(c_2) = 2^n - 2^j$ and $L_3(s^{(n)}) = 2^n - (2^p + 2^q)$, where $0 \leq p < q < n, L(c_3) = 2^n - 2^q$ or $L_3(s^{(n)}) = 2^n - (2^i + 2^j + 2^q)$, where $0 \leq q < n, q \neq i, j, L(c_3) = 2^n - 2^q$. Thus $j < q$.

In the case that $L_3(s^{(n)}) = 2^n - (2^p + 2^q)$, we now prove that $p \neq i, j$. Assume that $p = i$, and the distance (based on Definition 3.2.1 in Section 3.2) of nonzero elements p_1 and p_4 is 2^i, where p_1 is in c_1 (in the case that p_1 is in c_2, the proof is similar), p_4 is in c_3. As the distance of nonzero elements p_1 and p_2 is also 2^i, so the distance of nonzero elements p_2 and p_4 is 2^{i+1}, thus $L_3(s^{(n)}) = 2^n - (2^{i+1} + 2^q)$ should be true, which contradicts the fact that $L_3(s^{(n)}) = 2^n - (2^i + 2^q)$.

Assume that $p = j$, similarly one can prove that $L_3(s^{(n)}) = 2^n - (2^{j+1} + 2^q)$, which is not true, or one can prove that $L_3(s^{(n)}) = 2^n - (2^i + 2^j + 2^q)$. In this case, it is obvious that $q \neq i, j$.

Second, suppose that c_2 is a 2-cube and $L(c_2) = 2^n - (2^i + 2^j)$. It is easy to show that $L_1(s^{(n)}) = 2^n - (2^i + 2^j)$ and $L_3(s^{(n)}) = 2^n - (2^i + 2^j + 2^r), 0 \leq r < n, r \neq i, j$.

□

Next we investigate the distribution of $L_5(s^{(n)})$.

Theorem 4.3.2 Let $s^{(n)}$ be a 2^n-periodic binary sequence with linear complexity 2^n and

$L_5(s^{(n)}) < L_3(s^{(n)}) < L_1(s^{(n)})$, $L_1(s^{(n)}) = 2^n - (2^i + 2^j), 0 \le i < j < n$.

i). If $L_3(s^{(n)}) = 2^n - (2^p + 2^q), 0 \le p < q < n, j < q, p \ne i, j$, then $L_5(s^{(n)})$ can be $2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m}) < 2^n - (2^p + 2^q)$, where $0 \le i_1 < i_2 < \cdots < i_m < n, m > 3$.

For the case of $m = 3$. If $j < p$ or $i < p < j$, $\{i_1, i_2, i_3\} \ne \{i, p, q\}$; if $i > p$, $\{i_1, i_2, i_3\} \ne \{i, p, q\}$ and $\{j, p, q\}$. For the case of $m = 2$, $\{i_1, i_2\}$ can not include i, j, p or q.

ii). If $L_3(s^{(n)}) = 2^n - (2^i + 2^j + 2^r), 0 \le r < n, r \ne i, j$, then $L_5(s^{(n)})$ should be $2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m}) < 2^n - (2^p + 2^q)$, where $0 \le i_1 < i_2 < \cdots < i_m < n, m > 3$.

For the case of $m = 3$, $\{i_1, i_2, i_3\}$ can not contain $\{i, j\}$. For the case of $m = 2$, $\{i_1, i_2\}$ can not include i, j or r.

Proof. The following proof is based on the framework: $S + E = \{t + e | t \in S, e \in E\}$ (see definition in Chapter 2).

i). In the case that $L_5(s^{(n)}) = 2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m}) < 2^n - (2^i + 2^j), m > 3$, let $s^{(n)}$ be a 2^n-periodic binary sequence with linear complexity 2^n, $L_1(s^{(n)}) = 2^n - (2^i + 2^j)$ and $L_3(s^{(n)}) = 2^n - (2^p + 2^q)$.

Let $S = \{t | L(t) = 2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m})\}, E = \{e | W_H(e) = 5\}, S + E = \{t + e | t \in S, e \in E\}$, where t is a sequence with linear complexity $2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m})$ and e is a sequence with $W_H(e) = 5$. With the sieve method, we aim to sieve sequences $t + e$ with $L_5(t + e) = 2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m})$ from $S + E$.

We investigate the case that $s + u \in S + E$, but $L_5(t + u) < 2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m})$. This is equivalent to checking if there exists a sequence $v \in E$ such that $L(u + v) = 2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m}), m \ge 4$. As a 4-cube has $2^4 = 16$ nonzero elements and $W_H(u) = W_H(v) = 5$, thus it is impossible that $L(u+v) = 2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m}), m \ge 4$. Therefore, $L_5(s^{(n)})$ should be $2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m}) < 2^n - (2^p + 2^q)$.

Second we consider the case that $m = 3$ and $i > p$.

Let $s^{(n)}$ be a 2^n-periodic binary sequence with linear complexity 2^n. If $L_1(s^{(n)}) = 2^n - (2^i + 2^j)$ and $L_3(s^{(n)}) = 2^n - (2^p + 2^q)$, then $L_5(s^{(n)}) \ne 2^n - (2^p + 2^i + 2^q)$.

We will prove it by contradiction. Suppose that $L_5(s^{(n)}) = 2^n - (2^p + 2^i + 2^q)$. Let $S = \{t | L(t) = 2^n - (2^p + 2^i + 2^q)\}, E = \{e | W_H(e) = 5\}, S + E = \{t + e | t \in S, e \in E\}$, where

t is a sequence with linear complexity $2^n-(2^p+2^i+2^q)$ and e is a sequence with $W_H(e)=5$. With the sieve method, we aim to sieve sequences $t+e$ with $L_5(t+e)=2^n-(2^p+2^i+2^q)$ from $S+E$.

We now investigate the case that $s+u \in S+E$, but $L_5(t+u) < 2^n-(2^p+2^i+2^q)$. This is equivalent to checking if there exists a sequence $v \in E$ such that $L(u+v) = 2^n-(2^p+2^i+2^q)$.

For any $u \in E$ such that $L_1(t+u)=2^n-(2^i+2^j)$ and $L_3(t+u)=2^n-(2^p+2^q)$. There exists a sequence $v \in E$ such that $L_1(t+v)=2^n-(2^i+2^j)$, $L_3(t+v)=2^n-(2^p+2^q)$ and $L(u+v)=2^n-(2^p+2^i+2^q)$. So $L_5(t+u) < 2^n-(2^p+2^i+2^q)$. Therefore $\{i_1,i_2,i_3\} \neq \{i,p,q\}$.

(For example, let $u=\{1101\ 0100\ 1000\ 0000\}$ with $L(t)=2^4-(2^0+2^1+2^3)$, $L_1(t+u)=2^4-(2+2^2)$ and $L_3(t+u)=2^4-(1+2^3)$. There exists a sequence $v=\{0010\ 0100\ 0111\ 0000\}$ such that $L_1(t+v)=2^4-(2+2^2)$ and $L_3(t+v)=2^4-(1+2^3)$. As $L(u+v)=2^4-(2^0+2^1+2^3)$. So $L_5(t+u)<2^4-(2^0+2^1+2^3)$.)

Similarly, let $L(t)=2^n-(2^p+2^j+2^q)$. There exists a sequence $v \in E$ such that $L_1(t+v)=2^n-(2^i+2^j)$, $L_3(t+v)=2^n-(2^p+2^q)$ and $L(u+v)=2^n-(2^p+2^j+2^q)$. So $L_5(t+u)<2^n-(2^p+2^j+2^q)$. Therefore $\{i_1,i_2,i_3\} \neq \{j,p,q\}$.

In the case that $m=2$, $\{i_1,i_2\}$ can not include i,j,p or q. Suppose that $\{i_1,i_2\}$ comprises q and $L=2^n-(2^w+2^q)$. As $L=2^n-(2^w+2^q)<2^n-(2^p+2^q)$, thus $w>p$. Note that if the actual distance of two elements is 2^w-2^p, then the distance (see Definition 3.2.1 in Section 3.2) of these two elements is 2^p. We give the following example to illustrate the case.

Suppose that $n=5, i=2, j=3, p=1, q=4, w=2$,

$u^{(5)}=\{1010\ 0010\ 0010\ 0000\ 1000\ 0000\ 0000\ 0000\}$.

Then $L=2^n-(2^w+2^q)=12$. There exists

$v^{(5)}=\{0010\ 1010\ 0010\ 0000\ 0000\ 1000\ 0000\ 0000\}$, such that $L(u^{(5)}+v^{(5)})=2^5-(2^2+2^4)=12$. Therefore $L_5(s^{(n)}) \neq 2^n-(2^w+2^q)$.

ii). In the case that $m=3$ and $r>j$, we only give the following example to illustrate the proof.

In the case that $L_3(s^{(n)}) = 2^n - (2^i + 2^j + 2^r)$. Note that c_1 is a 0-cube and c_2 is a 2-cube, $L(c_2) = L_1(s^{(n)}) = 2^n - (2^i + 2^j)$. We also use the following example to illustrate the proof.

Suppose that $n = 4, i = 0, j = 1, r = 2$, $u^{(4)} = \{1111\ 1000\ 0000\ 0000\}$.

Then there exists $v^{(4)} = \{0000\ 1000\ 1111\ 0000\}$, such that $L(u^{(4)} + v^{(4)}) = 2^4 - (1 + 2 + 2^3)$. Therefore $L_5(s^{(n)}) \neq 2^n - (2^i + 2^j + 2^w) < 2^n - (2^i + 2^j + 2^r)$.

Similarly, for the case of $m = 2$, it is easy to show that $\{i_1, i_2\}$ can not include i, j or r.

This completes the proof. □

We next derive the counting formula of binary sequences with the prescribed 1-error linear complexity, the prescribed 3-error linear complexity and the prescribed 5-error linear complexity.

Theorem 4.3.3 Let $s^{(n)}$ be a 2^n-periodic binary sequence with linear complexity 2^n.

1) Suppose that $L_5(s^{(n)}) < L_3(s^{(n)}) < L_1(s^{(n)})$ and $L_1(s^{(n)}) = 2^n - (2^i + 2^j), 0 \leq i < j < n$, $L_3(s^{(n)}) = 2^n - (2^p + 2^q), 0 \leq p < q < n, j < q, p \neq i, j$, and $L_5(s^{(n)}) = 2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m}) < L_3(s^{(n)})$, where $0 \leq i_1 < i_2 < \cdots < i_m < n, m > 1$. Then the number of 2^n-periodic binary sequences $s^{(n)}$ can be given by

$$\delta \times 2^{5n-q-p-j-i-6} \times 2^{L-1}/(\theta \times \mu \times 2^{\epsilon} \times 32^{n-i_m-1})$$

where θ is defined in (4.1) of the following proof, δ, μ and ϵ are defined in the following proof according to $j < p$, $i < p < j$ and $p < i < j$.

If $L_5(s^{(n)}) = 0$, then the number of 2^n-periodic binary sequences $s^{(n)}$ can be given by

$$\gamma \times 2^{5n-q-p-j-i-6}$$

where if $j < p$ then $\gamma = 3$, if $j > p > i$ then $\gamma = 2$ else $\gamma = 1$.

2) Suppose that $L_5(s^{(n)}) < L_3(s^{(n)}) < L_1(s^{(n)})$ and $L_1(s^{(n)}) = 2^n - (2^i + 2^j), 0 \leq i < j < n$, $L_3(s^{(n)}) = 2^n - (2^i + 2^j + 2^r), 0 \leq r < n, r \neq i, j$, and $L_5(s^{(n)}) = 2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m}) < L_3(s^{(n)})$, where $0 \leq i_1 < i_2 < \cdots < i_m < n, m > 1$. Then the number of 2^n-periodic binary sequences $s^{(n)}$ can be given by

$$\delta \times 2^{5n-r-2j-i-6} \times 2^{L-1}/(\theta \times 2^{\epsilon} \times 32^{n-i_m-1})$$

where δ, θ and ϵ are defined in the following proof according to $j < r$, $i < r < j$ and $r < i < j$.

If $L_5(s^{(n)}) = 0$, then the number of 2^n-periodic binary sequences $s^{(n)}$ can be given by

$$\gamma \times 2^{5n-r-2j-i-6}$$

where if $r < i$ then $\gamma = 1/2$ else $\gamma = 1$.

Proof. 1) Let $S = \{t|L(t) = L\}, E = \{e|W_H(e) = 5\}, SE = \{t + e|t \in S, e \in E\}$, where t is a sequence with linear complexity $L = 2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m}), m > 2$ and e is a sequence with $W_H(e) = 5$, $L_1(e) = 2^n - (2^i + 2^j)$ and $L_3(e) = 2^n - (2^p + 2^q)$. With the sieve method, we aim to sieve sequences $t + e$ with $L_5(t + e) = L$ from $S + E$.

By Lemma 2.1.6 in Section 2.1, we know that the number of 2^n-periodic binary sequences t with $L(t) = L$ is 2^{L-1}. Now we will compute the number of sequences e with $W_H(e) = 5$, $L_1(e) = 2^n - (2^i + 2^j)$ and $L_3(e) = 2^n - (2^p + 2^q), j < q$.

In the case of $i < j < p < q$. The number of 2^{j+1}-periodic binary sequences $e^{(j+1)}$ with linear complexity $2^{j+1} - 2^j = 2^j$ and $W_H(e^{(j+1)}) = 2$ is 2^j. First one nonzero element is added so that $L_1(e^{(j+1)}) = 2^{j+1} - (2^i + 2^j)$. The number of $e^{(j+1)}$ becomes $2^j \times 2^{j-i}$.

Second one 1-cube with linear complexity $2^{q+1} - 2^q$ is added so that $L_3(e^{(q+1)}) = 2^{q+1} - (2^p + 2^q)$. Note that for $i = 0, j = 1, p = 2, q = 3$, sequence $\{1110\ 0100\}$ is from both $\{1110\ 0000\}$ and $\{1010\ 0100\}$. At the same time from sequence $\{1110\ 0100\}$, we have both $\{1110\ 0100\ 0100\ 0000\}$ and $\{1110\ 0100\ 0000\ 0100\}$ with $L_3(e^{(q+1)}) = 2^{q+1} - (2^p + 2^q)$. So the number of $e^{(q+1)}$ becomes $2^{2j-i} \times (2^3)^{p-j} \times 3 \times (2^4)^{q-p-1} \times 2^3 = 3 \times 2^{4q-p-j-i-1}$.

Finally the number of sequences $e^{(n)}$ with $W_H(e^{(n)}) = 5$, $L_1(e^{(n)}) = 2^n - (2^i + 2^j)$ and $L_3(e^{(n)}) = 2^n - (2^p + 2^q)$ can be given by

$$3 \times 2^{4q-p-j-i-1} \times (2^5)^{n-q-1} = 3 \times 2^{5n-q-p-j-i-6}.$$

In the case of $i < p < j < q$. One 1-cube with linear complexity $2^{q+1} - 2^q$ is added so that $L_3(e^{(q+1)}) = 2^{q+1} - (2^p + 2^q)$. The number of $e^{(q+1)}$ becomes $2^{2j-i} \times 2 \times 2^{j-p} \times (2^4)^{q-j-1} \times 2^3 = 2 \times 2^{4q-p-j-i-1}$.

Thus the number of sequences $e^{(n)}$ can be given by

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

In the case of $p < i < j < q$. One 1-cube with linear complexity $2^{q+1} - 2^q$ is added so that $L_3(e^{(q+1)}) = 2^{q+1} - (2^p + 2^q)$. The number of $e^{(q+1)}$ becomes $2^{2j-i} \times 2^{j-p} \times (2^4)^{q-j-1} \times 2^3 = 2^{4q-p-j-i-1}$.

Thus the number of sequences $e^{(n)}$ can be given by

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

In general, the number of these $e^{(n)}$ can be given by

$$\gamma \times 2^{5n-q-p-j-i-6}$$

where if $j < p$ then $\gamma = 3$, if $j > p > i$ then $\gamma = 2$ else $\gamma = 1$.

(The following example is given to illustrate the case of $j < p$.

Suppose that $n = 4, i = 0, j = 1, p = 2, q = 3$. From $v^{(4)} = \{0000\ 0001\ 0001\ 1111\}$, we can have the following.

$u_1^{(4)} = \{0000\ 0001\ 0001\ 1101\}$,

$u_2^{(4)} = \{0000\ 0001\ 0001\ 1011\}$,

$u_3^{(4)} = \{0000\ 0001\ 0001\ 1011\}$.

From $u_1^{(4)} = \{0000\ 0001\ 0001\ 1101\}$, we can also have the following.

$u_{11}^{(4)} = \{0000\ 1001\ 0001\ 0101\}$,

$u_{12}^{(4)} = \{0000\ 0101\ 0001\ 1001\}$,

$u_{13}^{(4)} = \{0000\ 1101\ 0001\ 0001\}$.)

We now investigate the case that $s + u, t + v \in S + E$ and $L_5(s + u) = L_5(t + v) = L$ with $s \neq t$, $u \neq v$, but $s + u = t + v$. It is equivalent to checking if there exists a sequence v such that $L(u + v) = L(s + t) < L$ and if so, check the number of such sequence v, where $W_H(u) = W_H(v) = 5$. We need to consider the following two cases.

The first case is related to the minimum $i_0 < q$ such that $2^n - (2^{i_0} + 2^q) < L = 2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m})$, where $q = i_m$. If $p < i, j$, then i_0 can be i or j.

For any $u \in E$, it is easy to show that there exist $2^{q-i_0} - 1$ sequences v, such that $L(u+v) < L$.

(The following example is given to illustrate the above case.

Suppose that $n = 5, i = 0, j = 1, p = 2, q = 4,\ i_1 = 0, i_2 = 1, i_3 = 2, i_4 = 4$. So $L = 2^n - (2^{i_1} + 2^{i_2} + 2^{i_3} + 2^{i_4}) = 9$.

If $u^{(5)} = \{1000\ 1110\ 0000\ 0000\ 1000\ 0000\ 0000\ 0000\}$, then

$v^{(5)} = \{0000\ 1110\ 1000\ 0000\ 0000\ 0000\ 1000\ 0000\}$.

Thus $L(u^{(5)} + v^{(5)}) = 2^5 - (2^3 + 2^4) = 8, i_0 = 3.$)

Second we consider the case of $i_m < w < n$.

Suppose that $j < p$. For $i_m < w < n$, there exist $31 \times 32^{w-i_m-1}$ sequences v, such that $L(u+v) = 2^n - (2^q + 2^w) < L$ or $L(u+v) = 2^n - (2^p + 2^w) < L$ or $L(u+v) = 2^n - (2^j + 2^w) < L$ or $L(u+v) = 2^n - (2^i + 2^w) < L$ or $L(u+v) = 2^n - 2^w < L$.

Note that for any sequence v with 5 nonzero elements, if we double the period of sequence v, then 2^5 new sequences will be generated. Therefore there exist

$$31 + 31 \times 32 + \cdots + 31 \times 32^{n-i_m-2} = 32^{n-i_m-1} - 1$$

sequences v, such that $L(u+v) < L$.

(The following example is given to illustrate the above case.

Suppose that $n = 5, i = 0, j = 1, p = 2, q = 3, i_1 = 1, i_2 = 2, i_3 = 3, w = 4$,

$u^{(5)} = \{1011\ 1000\ 1000\ 0000\ 0000\ 0000\ 0000\ 0000\}$. Then

$v_1^{(5)} = \{0011\ 1000\ 0000\ 0000\ 1000\ 0000\ 1000\ 0000\}$.

Thus $L(u^{(5)} + v_1^{(5)}) = 2^5 - (2^3 + 2^4)$.

$v_2^{(5)} = \{0011\ 0000\ 1000\ 0000\ 1000\ 1000\ 0000\ 0000\}$,

$v_3^{(5)} = \{1011\ 0000\ 0000\ 0000\ 0000\ 1000\ 1000\ 0000\}$,

Thus $L(u^{(5)}+v_2^{(5)}) = L(u^{(5)}+v_3^{(5)}) = 2^5-(2^2+2^4)$.

$v_4^{(5)} = \{0001\ 1000\ 1000\ 0000\ 1010\ 0000\ 0000\ 0000\}$,

$v_5^{(5)} = \{1001\ 0000\ 1000\ 0000\ 0010\ 1000\ 0000\ 0000\}$,

$v_6^{(5)} = \{1001\ 1000\ 0000\ 0000\ 0010\ 0000\ 1000\ 0000\}$,

$v_7^{(5)} = \{0001\ 0000\ 0000\ 0000\ 1010\ 1000\ 1000\ 0000\}$.

Thus $L(u^{(5)}+v_4^{(5)}) = L(u^{(5)}+v_5^{(5)}) = L(u^{(5)}+v_6^{(5)}) = L(u^{(5)}+v_7^{(5)}) = 2^5-(2+2^4)$.

.....

$v_{31}^{(5)} = \{0011\ 1000\ 1000\ 0000\ 1000\ 0000\ 0000\ 0000\}$.

Thus $L(u^{(5)}+v_{31}^{(5)}) = 2^5-2^4$.)

On the other hand, if $q < i_m$ and only $2^n-(2^q+2^{i_m}) < L$ then the number of v will be increased by 32^{n-i_m-1}.

If $2^n-(2^p+2^{i_m}) < L$ and $2^n-(2^j+2^{i_m}) > L$ then the number of v will be increased by $3\times 32^{n-i_m-1}$.

If $2^n-(2^j+2^{i_m}) < L$ and $2^n-(2^i+2^{i_m}) > L$ then the number of v will be increased by $7\times 32^{n-i_m-1}$.

If $2^n-(2^i+2^{i_m}) < L$ then the number of v will be increased by $15\times 32^{n-i_m-1}$.

It follows that the number of 2^n-periodic binary sequences $s^{(n)}$ with $L(s^{(n)}) = 2^n$, $L_1(s^{(n)}) = 2^n-(2^i+2^j)$, $L_3(s^{(n)}) = 2^n-(2^p+2^q)$ and $L_5(s^{(n)}) = L$ can be given by

$$\delta\times 2^{5n-q-p-j-i-6}\times 2^{L-1}/(\theta\times\mu\times 2^{\epsilon}\times 32^{n-i_m-1})$$

where

$$\text{if } q=i_m \text{ and there exits } i_0<q \text{ then } \theta=2^{q-i_0} \text{ else } \theta=1. \tag{4.1}$$

For the case of $j < p$. If $L = 2^n-(2^j+2^p+2^q)$ then $\delta = 1$, if $L = 2^n-(2^i+2^p+2^q)$ then $\delta = 0$ else $\delta = 3$; if $L > 2^n-(2^i+2^p+2^q)$ then $\mu = 2$ else $\mu = 1$; if $q < i_m$ and only

$2^n - (2^q + 2^{i_m}) < L$ then $\epsilon = 1$, if $2^n - (2^p + 2^{i_m}) < L$ and $2^n - (2^j + 2^{i_m}) > L$ then $\epsilon = 2$, if $2^n - (2^j + 2^{i_m}) < L$ and $2^n - (2^i + 2^{i_m}) > L$ then $\epsilon = 3$, if $2^n - (2^i + 2^{i_m}) < L$ then $\epsilon = 4$.

(The following example is given to illustrate the case of $j < p$.

Suppose that $n = 4, i = 0, j = 1, p = 2, q = 3$, $L = 2^4 - (2^j + 2^p + 2^q)$. $u_1^{(4)} = \{1110\ 1000\ 1000\ 0000\}$.

There exists $v_1^{(4)} = \{0100\ 0010\ 0010\ 1010\}$, such that $L(u_1^{(4)} + v_1^{(4)}) = 2^4 - (2^j + 2^p + 2^q)$.

There exists $v_2^{(4)} = \{0010\ 0100\ 0100\ 1100\}$, such that $L(u_1^{(4)} + v_2^{(4)}) = 2^4 - (2^i + 2^p + 2^q)$.

For $u_2^{(4)} = \{1011\ 1000\ 1000\ 0000\}$.

There exists $v_1^{(4)} = \{0001\ 0010\ 0010\ 1010\}$, such that $L(u_2^{(4)} + v_1^{(4)}) = 2^4 - (2^j + 2^p + 2^q)$.

There exists $v_2^{(4)} = \{0010\ 0001\ 0001\ 1001\}$, such that $L(u_2^{(4)} + v_2^{(4)}) = 2^4 - (2^i + 2^p + 2^q)$.

For $u_3^{(4)} = \{1101\ 1000\ 1000\ 0000\}$. Then there exists $v_2^{(4)} = \{0001\ 0100\ 0100\ 1100\}$, such that $L(u_3^{(4)} + v_2^{(4)}) = 2^4 - (2^i + 2^p + 2^q) < L$, but there is no $v_1^{(4)}$ such that $W_H(v_1^{(4)}) = 5$ and $L(u_3^{(4)} + v_1^{(4)}) = L$.

So, suppose that $L(s^{(4)}) = L$. Then $L_5(s^{(4)} + u_3^{(4)}) = L$.)

For the case of $j > p > i$. If $L = 2^n - (2^j + 2^p + 2^q)$ then $\delta = 1$, if $L = 2^n - (2^i + 2^j + 2^q)$ then $\delta = 1/2$, if $L = 2^n - (2^i + 2^p + 2^q)$ then $\delta = 0$ else $\delta = 2$; if $L > 2^n - (2^i + 2^p + 2^q)$ then $\mu = 2$ else $\mu = 1$; if $q < i_m$ and only $2^n - (2^q + 2^{i_m}) < L$ then $\epsilon = 1$, if $2^n - (2^j + 2^{i_m}) < L$ and $2^n - (2^p + 2^{i_m}) > L$ then $\epsilon = 2$, if $2^n - (2^p + 2^{i_m}) < L$ and $2^n - (2^i + 2^{i_m}) > L$ then $\epsilon = 3$, if $2^n - (2^i + 2^{i_m}) < L$ then $\epsilon = 4$.

(The following example is given to illustrate the case of $j > p > i$.

Suppose that $n = 4, i = 0, j = 2, p = 1, q = 3$, $L = 2^n - (2^i + 2^j + 2^q)$, $u^{(4)} = \{1110\ 0010\ 1000\ 0000\}$.

Then there exists $v^{(4)} = \{0100\ 1000\ 0010\ 1010\}$, such that $L(u^{(4)} + v^{(4)}) = 2^4 - (2^j + 2^p + 2^q) < L$, but there is no $v_1^{(4)}$ such that $W_H(v_1^{(4)}) = 5$ and $L(u^{(4)} + v_1^{(4)}) = L$.

So, suppose that $L(s^{(4)}) = 2^n - (2^i + 2^j + 2^q)$. Then $L_5(s^{(4)} + u^{(4)}) = 2^n - (2^i + 2^j + 2^q)$.

There exists $v_2^{(4)} = \{0001\ 0010\ 0111\ 0000\}$, such that $L(u^{(4)} + v_2^{(4)}) = 2^4 - (2^i + 2^p + 2^q)$.)

For the case of $j > i > p$. If $L = 2^n - (2^j + 2^p + 2^q)$ or $L = 2^n - (2^i + 2^p + 2^q)$ then $\delta = 0$ else $\delta = 1$; if $L > 2^n - (2^i + 2^p + 2^q)$ and $L > 2^n - (2^j + 2^p + 2^q)$ then $\mu = 4$, if only $L > 2^n - (2^j + 2^p + 2^q)$ then $\mu = 2$ else $\mu = 1$; if $q < i_m$ and only $2^n - (2^q + 2^{i_m}) < L$ then $\epsilon = 1$, if $2^n - (2^j + 2^{i_m}) < L$ and $2^n - (2^i + 2^{i_m}) > L$ then $\epsilon = 2$, if $2^n - (2^i + 2^{i_m}) < L$ and $2^n - (2^p + 2^{i_m}) > L$ then $\epsilon = 3$, if $2^n - (2^p + 2^{i_m}) < L$ then $\epsilon = 4$.

(The following example is given to illustrate the case of $j > i > p$.

Suppose that $n = 4, i = 1, j = 2, p = 0, q = 3$, $L = 2^n - (2^i + 2^j + 2^q)$, $u^{(4)} = \{1101\ 0100\ 1000\ 0000\}$.

Then there exists $v^{(4)} = \{0010\ 0100\ 0111\ 0000\}$, such that $L(u^{(4)} + v^{(4)}) = 2^4 - (2^i + 2^p + 2^q)$.

There exists $v_1^{(4)} = \{0001\ 1000\ 0100\ 1100\}$, such that $L(u^{(4)} + v_1^{(4)}) = 2^4 - (2^j + 2^p + 2^q)$.

There is no $v_0^{(4)}$ such that $W_H(v_0^{(4)}) = 5$ and $L(u^{(4)} + v_0^{(4)}) = L$. So, suppose that $L(s^{(4)}) = 2^n - (2^i + 2^j + 2^q)$. Then $L_5(s^{(4)} + u^{(4)}) = 2^n - (2^i + 2^j + 2^q)$.)

2) First we consider the case of $i < j < r$. 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 3.1.1 in Section 3.1, 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}.

Thus the number of 2^{r+1}-periodic binary sequences $s^{(r+1)}$ with linear complexity $2^{r+1} - (2^r + 2^j + 2^i)$ and $W_H(s^{(r+1)}) = 8$ is $(2^4)^{r-j-1} \times 2^{2j-i-2} = 2^{4r-2j-i-6}$.

There exist 2^4 2-cubes with linear complexity $2^{r+1} - (2^j + 2^i)$ from one 3-cube with linear

complexity $2^{r+1}-(2^r+2^j+2^i)$. Any pair of one 2-cube with linear complexity $2^{r+1}-(2^j+2^i)$ and one vertex from the 3-cube is come from exactly two different 2-cubes.

(The following example is given to illustrate the above case.

Suppose that $n=4, i=0, j=1, r=3$, $u^{(4)}=\{1111\ 0000\ 1111\ 0000\}$. Then $L(u^{(4)})=2^4-(2^i+2^j+2^r)$.

There exist 2^4 2-cubes with linear complexity $2^{r+1}-(2^j+2^i)$, such as $\{0111\ 0000\ 1000\ 0000\}$. And $\{1111\ 0000\ 1000\ 0000\}$ is from both $\{1111\ 0000\ 0000\ 0000\}$ and $\{0111\ 0000\ 1000\ 0000\}$.)

As $u \in E$ such that $L_1(u)=2^n-(2^i+2^j)$ and $L_3(u)=2^n-(2^i+2^j+2^r)$. So the number of these u can be given by

$$2^3 \times 2^2 \times (2^5)^{n-r-1} \times 2^{4r-2j-i-6} = 2^{5n-r-2j-i-6}.$$

Secondly, we consider the case of $r<i<j$.

We know that the number of 2^n-periodic binary sequences $s^{(n)}$ with linear complexity $2^n-(2^j+2^i)$ and $W_H(s^{(n)})=4$ is $(2^4)^{n-j-1} \times 2^{2j-i-2} = 2^{4n-2j-i-6}$.

There exit $\frac{2^n}{2^{r+1}}$ locations with the distance 2^r (Definition 3.2.1 in Section 3.2) to every vertex in a 2-cube. As $u \in E$ such that $L_1(u)=2^n-(2^i+2^j)$ and $L_3(u)=2^n-(2^i+2^j+2^r)$. So the number of these u can be given by

$$\frac{2^n}{2^{r+1}} \times 2^{4n-2j-i-6} = 2^{5n-r-2j-i-7}.$$

Thirdly, we consider the case of $i<r<j$.

We know that the number of 2^n-periodic binary sequences $s^{(n)}$ with linear complexity $2^n-(2^j+2^i)$ and $W_H(s^{(n)})=4$ is $2^{4n-2j-i-6}$.

There exit $\frac{2^n}{2^{r+1}}$ locations with the distance 2^r to every two vertices in a 2-cube. As $u \in E$ such that $L_1(u)=2^n-(2^i+2^j)$ and $L_3(u)=2^n-(2^i+2^j+2^r)$. So the number of these u can be given by

$$\frac{2^n}{2^{r+1}} \times 2 \times 2^{4n-2j-i-6} = 2^{5n-r-2j-i-6}.$$

(The following example is given to illustrate the above case.

Suppose that $n = 4, i = 0, j = 3, r = 2$, $v^{(4)} = \{1100\ 0000\ 1100\ 0000\}$. Then $L(v^{(4)}) = 2^4 - (2^i + 2^j)$.

There exist 4 binary sequences u with $L_1(u) = 2^n - (2^i + 2^j)$ and $L_3(u) = 2^n - (2^i + 2^j + 2^r)$, such as

$\{1100\ 1000\ 1100\ 0000\}$,

$\{1100\ 0000\ 1100\ 1000\}$,

$\{1100\ 0100\ 1100\ 0000\}$,

$\{1100\ 0000\ 1100\ 0100\}$.)

We now investigate the case that $s + u, t + v \in S + E$ and $L_5(s + u) = L_5(t + v) = L$ with $s \neq t$, $u \neq v$, but $s + u = t + v$. We need to consider the following two cases.

The first case is related to the minimum $i_0 < j$ such that $2^n - (2^{i_0} + 2^i + 2^j) < L = 2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m})$. Suppose that $j = i_m$ and $r < i$, $i_0 < i$. For any $u \in E$, it is easy to show that there exist $2^{j-i_0-1} - 1$ sequences v, such that $L(u + v) < L$.

(The following example is given to illustrate the above case.

Suppose that $n = 5, i = 3, j = 4, r = 1$, $i_1 = 0, i_2 = 1, i_3 = 3, i_4 = 4$. So $L = 2^n - (2^{i_1} + 2^{i_2} + 2^{i_3} + +2^{i_4}) = 5$.

If $u^{(5)} = \{1010\ 0000\ 1000\ 0000\ 1000\ 0000\ 1000\ 0000\}$, then

$v^{(5)} = \{0010\ 1000\ 0000\ 1000\ 0000\ 1000\ 0000\ 1000\}$.

Thus $L(u^{(5)} + v^{(5)}) = 2^5 - (2^2 + 2^3 + 2^4) = 4, i_0 = 2$.)

Suppose that $j = i_m$ and $i < r < j$, $i < i_0 < j$. For any $u \in E$, it is easy to show that there exist $2^{j-i_0} - 1$ sequences v, such that $L(u + v) < L$.

The second case is related to $i_m < w < n$.

Suppose that $j < r$. For $i_m < w < n$, there exist $31 \times 32^{w-i_m-1}$ sequences v, such that $L(u + v) = 2^n - (2^r + 2^w) < L$ or $L(u + v) = 2^n - (2^i + 2^j + 2^w) < L$ or $L(u + v) =$

$2^n - (2^j + 2^w) < L$ or $L(u+v) = 2^n - (2^i + 2^w) < L$ or $L(u+v) = 2^n - 2^w < L$.

Note that for any sequence v with 5 nonzero elements, if we double the period of sequence v, then 2^5 new sequences will be generated. Therefore there exist

$$31 + 31 \times 32 + \cdots + 31 \times 32^{n-i_m-2} = 32^{n-i_m-1} - 1$$

sequences v, such that $L(u+v) < L$.

(The following example is given to illustrate the above case.

Suppose that $n = 5, i = 0, j = 1, r = 2, i_1 = 1, i_2 = 2, i_3 = 3, w = 4$,

$u^{(5)} = \{1111\ 1000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\}$. Then

$v_1^{(5)} = \{0111\ 0000\ 0000\ 0000\ 1000\ 1000\ 0000\ 0000\}$.

Thus $L(u^{(5)} + v_1^{(5)}) = 2^5 - (2^2 + 2^4)$.

$v_2^{(5)} = \{0000\ 1000\ 0000\ 0000\ 1111\ 0000\ 0000\ 0000\}$,

$v_3^{(5)} = \{1000\ 0000\ 0000\ 0000\ 0111\ 1000\ 0000\ 0000\}$,

Thus $L(u^{(5)} + v_2^{(5)}) = L(u^{(5)} + v_3^{(5)}) = 2^5 - (1 + 2 + 2^4)$.

$v_4^{(5)} = \{0101\ 1000\ 0000\ 0000\ 1010\ 0000\ 0000\ 0000\}$,

$v_5^{(5)} = \{1010\ 1000\ 0000\ 0000\ 0101\ 0000\ 0000\ 0000\}$,

$v_6^{(5)} = \{1101\ 0000\ 0000\ 0000\ 0010\ 1000\ 0000\ 0000\}$,

$v_7^{(5)} = \{0010\ 0000\ 0000\ 0000\ 1101\ 1000\ 0000\ 0000\}$.

Thus $L(u^{(5)} + v_4^{(5)}) = L(u^{(5)} + v_5^{(5)}) = L(u^{(5)} + v_6^{(5)}) = L(u^{(5)} + v_7^{(5)}) = 2^5 - (2 + 2^4)$.

.....

$v_{31}^{(5)} = \{0000\ 0000\ 0000\ 0000\ 1111\ 1000\ 0000\ 0000\}$.

Thus $L(u^{(5)} + v_{31}^{(5)}) = 2^5 - 2^4$.)

On the other hand, if $r < i_m$ and only $2^n - (2^r + 2^{i_m}) < L$ then the number of v will be increased by 32^{n-i_m-1}.

If $2^n - (2^i + 2^j + 2^{i_m}) < L$ and $2^n - (2^j + 2^{i_m}) > L$ then the number of v will be increased by $3 \times 32^{n-i_m-1}$.

If $2^n - (2^j + 2^{i_m}) < L$ and $2^n - (2^i + 2^{i_m}) > L$ then the number of v will be increased by $7 \times 32^{n-i_m-1}$.

If $2^n - (2^i + 2^{i_m}) < L$ then the number of v will be increased by $15 \times 32^{n-i_m-1}$.

It follows that the number of 2^n-periodic binary sequences $s^{(n)}$ with $L(s^{(n)}) = 2^n$, $L_1(s^{(n)}) = 2^n - (2^i + 2^j)$, $L_3(s^{(n)}) = 2^n - (2^i + 2^j + 2^r)$ and $L_5(s^{(n)}) = L$ can be given by

$$\delta \times 2^{5n-r-2j-i-6} \times 2^{L-1}/(\theta \times 2^{\epsilon} \times 32^{n-i_m-1})$$

For the case of $j < r$. $\delta = 1, \theta = 1$. If $r < i_m$ and only $2^n - (2^r + 2^{i_m}) < L$ then $\epsilon = 1$, if $2^n - (2^i + 2^j + 2^{i_m}) < L$ and $2^n - (2^j + 2^{i_m}) > L$ then $\epsilon = 2$, if $2^n - (2^j + 2^{i_m}) < L$ and $2^n - (2^i + 2^{i_m}) > L$ then $\epsilon = 3$, if $2^n - (2^i + 2^{i_m}) < L$ then $\epsilon = 4$.

For the case of $i < r < j$. $\delta = 1$. If $j = i_m$ and $i < i_0 < j$ then $\theta = 2^{j-i_0}$ else $\theta = 1$. If $j < i_m$ and only $2^n - (2^i + 2^j + 2^{i_m}) < L$ then $\epsilon = 1$, if $2^n - (2^j + 2^{i_m}) < L$ and $2^n - (2^r + 2^{i_m}) > L$ then $\epsilon = 2$, if $2^n - (2^r + 2^{i_m}) < L$ and $2^n - (2^i + 2^{i_m}) > L$ then $\epsilon = 3$, if $2^n - (2^i + 2^{i_m}) < L$ then $\epsilon = 4$.

For the case of $r < i < j$. $\delta = 1/2$. If $j = i_m$ and $i_0 < i$ then $\theta = 2^{j-i_0-1}$ else $\theta = 1$. If $j < i_m$ and only $2^n - (2^i + 2^j + 2^{i_m}) < L$ then $\epsilon = 1$, if $2^n - (2^j + 2^{i_m}) < L$ and $2^n - (2^i + 2^{i_m}) > L$ then $\epsilon = 2$, if $2^n - (2^i + 2^{i_m}) < L$ and $2^n - (2^r + 2^{i_m}) > L$ then $\epsilon = 3$, if $2^n - (2^r + 2^{i_m}) < L$ then $\epsilon = 4$.

The proof is complete. □

To further illustrate Theorem 4.3.3, we give the following two examples, which are verified by a computer program as well.

Example 4.3.1 Suppose that $n = 5, i = 0, j = 1, p = 2, q = 4$, $i_1 = 0, i_2 = 1, i_3 = 2, i_4 = 4$. So $L = 2^n - (2^{i_1} + 2^{i_2} + 2^{i_3} + 2^{i_4}) = 9$. As $j < p$ and $q = i_4$, so $\delta = 3$, $i_0 = 3$, $\theta = 2^{q-i_0} = 2$, $\epsilon = 0$. The number of 2^5-periodic binary sequences $s^{(5)}$ with $L(s^{(5)}) = 32$,

$L_1(s^{(5)}) = 29$, $L_3(s^{(5)}) = 12$ and $L_5(s^{(5)}) = 9$ can be given by

$$(3 \times 2^{5\times n-4-2-1-6}) \times 2^{9-1}/(2 \times 32^{5-4-1}) = 3 \times 2^{19}.$$

Example 4.3.2 Suppose that $n = 5, i = 3, j = 4, r = 1$, $i_1 = 0, i_2 = 1, i_3 = 3, i_4 = 4$. So $L = 2^n - (2^{i_1} + 2^{i_2} + 2^{i_3} + 2^{i_4}) = 5$. As $r < i$ and $j = i_4$, so $i_0 = 2$, $\delta = 1/2$, $\theta = 2^{j-i_0-1} = 2$, $\epsilon = 0$. The number of 2^5-periodic binary sequences $s^{(5)}$ with $L(s^{(5)}) = 32$, $L_1(s^{(5)}) = 8$, $L_3(s^{(5)}) = 6$ and $L_5(s^{(5)}) = 5$ can be given by

$$(\frac{1}{2} \times 2^{5\times n-1-8-3-6}) \times 2^{5-1}/(2 \times 32^{5-4-1}) = 2^9.$$

4.4 A constructive approach for computing descent points of the k-error linear complexity

How many elements have to be changed to decrease the linear complexity? For a 2^n-periodic binary sequence $s^{(n)}$, Kurosawa *et al.* (2000) showed that the first descent point of the k-error linear complexity is reached by $k = 2^{W_H(2^n - L(s^{(n)}))}$, where $W_H(a)$ denotes the Hamming weight of the binary representation of an integer a.

In this section, first, the k-error cube decomposition of 2^n-periodic binary sequences is developed based on the proposed cube theory. Second we investigate the formula to determine the second descent points for the k-error linear complexity of 2^n-periodic binary sequences based on the linear complexity and the first descent points for the k-error linear complexity. Third we study the formula to determine the third descent points for the k-error linear complexity based on the linear complexity, the first and second descent points for the k-error linear complexity.

For clarity of presentation, we first introduce some definitions.

Let $k^{(i)}$ denote the ith descent point of the k-error linear complexity, where $i > 0$. We define $S(a)$ as the binary representation of an integer a, and $W_H(S(a))$ denotes the Hamming weight of $S(a)$. We further define $L^{(i)}(s^{(n)})$ as the k-error linear complexity of the ith descent point for a 2^n-periodic binary sequence $s^{(n)}$, and define

$$S(s^{(n)}) = S(2^n - L(s^{(n)}))$$

$$S^{(i)}(s^{(n)}) = S(2^n - L^{(i)}(s^{(n)}))$$

where $i \geq 0$ and $L(s^{(n)})$ is also denoted as $L^{(0)}(s^{(n)})$. For a given binary digit representation S_1, one can prove easily that there exists only one linear complexity value $L_1 = 2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m})$, where $0 \leq i_1 < i_2 < \cdots < i_m < n$, such that $S_1 = S(2^n - L_1)$. In this case, we define

$$S^{-1}(S_1) = i_1, S^{-m}(S_1) = i_m$$

$$S_{>i_k}(2^n - L_1) = S(2^{i_{k+1}} + 2^{i_{k+2}} + \cdots + 2^{i_m})$$

Let $S(a) = (x_1, x_2, \cdots, x_n)$ and $S(b) = (y_1, y_2, \cdots, y_n)$. Then define $S(a) \cap S(b) = (x_1 y_1, x_2 y_2, \cdots, x_n y_n)$, $S(a) \cup S(b) = (x_1 + y_1 - x_1 y_1, x_2 + y_2 - x_2 y_2, \cdots, x_n + y_n - x_n y_n)$.

To obtain our main results, we first present the following lemma.

Lemma 4.4.1 Let $s^{(n)}$ be a 2^n-periodic binary sequence. Assume that the second last decent point of k-error linear complexity of $s^{(n)}$ is $(k^{(j)}, L^{(j)}(s^{(n)}))$. Then $L^{(j)}(s^{(n)})$ is achieved by a cube $c^{(j)}$ exactly.

Proof. Suppose that the last decent point of k-error linear complexity is $(k^{(j+1)}, L^{(j+1)}(s^{(n)}))$. Then $L^{(j+1)}(s^{(n)}) = 0$. Assume that the second last decent point of k-error linear complexity is $(k^{(j)}, L^{(j)}(s^{(n)}))$.

By Algorithm 2.2, $s^{(n)}$ has a standard cube decomposition. Let $s^{(n)} = c_1 + c_2 + \cdots + c_m$, where $L(c_1) > L(c_2) > \cdots > L(c_m)$.

By the definition of k-error linear complexity, the smallest k-error linear complexity greater than 0 is achieved by a cube $c^{(j)}$, which can be constructed by c_m, some nonzero elements of $c_1, c_2, \cdots, c_{m-1}$ and adding some new nonzero elements to $s^{(n)}$. Other nonzero elements of $c_1, c_2, \cdots, c_{m-1}$ will be changed to zero.

Suppose that there are x nonzero elements in c_m, the number of nonzero elements of $c_1, c_2, \cdots, c_{m-1}$ used by $c^{(j)}$ is y, and the number of nonzero elements of $c_1, c_2, \cdots, c_{m-1}$ not used by $c^{(j)}$ is z, where $x > y > 0, z \geq 0$. To construct $c^{(j)}$, one has to add a 2^n-periodic binary sequence $e_j^{(n)}$ to $s^{(n)}$, where $e_j^{(n)}$ has $x - y + z$ nonzero elements. Note that the number of nonzero elements in $s^{(n)}$ is $x + y + z$. So $x - y + z < x + y + z$. Thus $c^{(j)}$ has the smallest k-error linear complexity greater than 0. □

It is easy to see that $c^{(j)}$ is not unique for some 2^n-periodic binary sequences. For example, let $s^{(3)} = \{1110\ 0000\}$. Then $c^{(j)}$ can be $\{1111\ 0000\}$ or $\{1110\ 0001\}$.

Based on Lemma 4.4.1, next we present a very fundamental theorem regarding the CELCS, followed by an important definition called **the k-error cube decomposition**.

Theorem 4.4.1 Let $s^{(n)}$ be a 2^n-periodic binary sequence. Then

i) we have a decomposition $s^{(n)} = c^{(0)}+c^{(1)}+c^{(2)}+\cdots+c^{(j)}$, where $c^{(i)}$ is a cube with linear complexity $L(c^{(i)}) = L^{(i)}(s^{(n)})$, the second last decent point of k-error linear complexity of $s^{(n)}$ is $(k^{(j)}, L^{(j)}(s^{(n)}))$ and $k^{(i+1)} = W_H(c^{(0)} + c^{(1)} + c^{(2)} + \cdots + c^{(i)}), 0 \le i \le j$;

ii) we have a decomposition $s^{(n)} = c^{(0)} + c^{(1)} + c^{(2)} + \cdots + c^{(m)} + t_m^{(n)}$, where $c^{(i)}$ is a cube with linear complexity $L(c^{(i)}) = L^{(i)}(s^{(n)})$, $t_m^{(n)}$ is a 2^n-periodic binary sequence with $L^{(m)}(s^{(n)}) > L(t_m^{(n)})$, and $k^{(m+1)} \le W_H(c^{(0)} + c^{(1)} + c^{(2)} + \cdots + c^{(m)})$.

Proof. i) Assume that the second last decent point of k-error linear complexity is $(k^{(j)}, L^{(j)}(s^{(n)}))$, and $L^{(j)}(s^{(n)})$ is achieved with a cube $c^{(j)}$ by adding a 2^n-periodic binary sequence $e_j^{(n)}$ to $s^{(n)}$, where $k^{(j)} = W_H(e_j^{(n)})$. Thus $e_j^{(n)} + s^{(n)} = c^{(j)}$, which implies that $s^{(n)} = e_j^{(n)} + c^{(j)}$.

By the definition of k-error linear complexity, $W_H(e_j^{(n)}) < W_H(s^{(n)})$.

$e_j^{(n)}$ is also a 2^n-periodic binary sequence. Similarly, $e_j^{(n)} = e_{j-1}^{(n)} + c^{(j-1)}$, and $W_H(e_{j-1}^{(n)}) < W_H(e_j^{(n)})$. If $L(c^{(j-1)}) \le L(c^{(j)})$, as $s^{(n)} = e_j^{(n)}+c^{(j)} = e_{j-1}^{(n)}+c^{(j-1)}+c^{(j)}$, then adding a 2^n-periodic binary sequence $e_{j-1}^{(n)}$ to $s^{(n)}$, in this case $L(e_{j-1}^{(n)}+s^{(n)}) < L(c^{(j)})$. This contradicts the fact that $k^{(j)} = W_H(e_j^{(n)})$. Thus $L(c^{(j-1)}) > L(c^{(j)})$ and $k^{(j-1)} = W_H(e_{j-1}^{(n)})$.

.....

Finally, based on the above analysis, we have that $s^{(n)} = c^{(0)}+c^{(1)}+c^{(2)}+\cdots+c^{(j)}$, where $L(c^{(0)}) > L(c^{(1)}) > L(c^{(2)}) > \cdots > L(c^{(j)})$, $L^{(i)}(s^{(n)}) = L(c^{(i)})$, and $k^{(i)} = W_H(e_i^{(n)}) = W_H(c^{(0)} + c^{(1)} + c^{(2)} + \cdots + c^{(i-1)}), 0 \le i \le j+1$.

ii) In the case of i), we first obtain the last cube $c^{(j)}$, then $c^{(j-1)}$, $c^{(j-2)}$, ...

In this case, we first obtain the cube $c^{(m)}$, so that $L^{(m)}(s^{(n)}) = L(c^{(m)})$.

Assume that $L^{(m)}(s^{(n)})$ is achieved with a cube $c^{(m)}$ by adding a 2^n-periodic binary sequence $e_m^{(n)}$ to $s^{(n)}$, which implies that $s^{(n)} = e_m^{(n)} + c^{(m)} + t_m^{(n)}$, where $L(t_m^{(n)}) < L(c^{(m)})$.

By applying the result of i) to $e_m^{(n)}$, we have that $s^{(n)} = c^{(0)} + c^{(1)} + c^{(2)} + \cdots + c^{(m)} + t_m^{(n)}$, where $L(c^{(i)}) = L^{(i)}(s^{(n)})$, $k^{(i)} = W_H(e_i^{(n)}) = W_H(c^{(0)} + c^{(1)} + c^{(2)} + \cdots + c^{(i-1)}), 0 \leq i \leq m$.

It is obvious that $k^{(m+1)} \leq W_H(c^{(0)} + c^{(1)} + c^{(2)} + \cdots + c^{(m)})$. □

Next we give some examples in different situations to illustrate Theorem 4.4.1.

Example 4.4.1 In fact, there indeed exists the case that $k^{(m+1)} < W_H(c^{(0)} + c^{(1)} + c^{(2)} + \cdots + c^{(m)})$. Let
$c^{(0)} = \{11001100\ 00000000\ 00000000\ 00000000\}$,
$c^{(1)} = \{10101010\ 10101010\ 00000000\ 00000000\}$,
$c^{(2)} = \{11001100\ 11001100\ 11001100\ 11001100\}$,
$t_2^{(5)} = \{11111111\ 11111111\ 11111111\ 11111111\}$,
and $s^{(5)} = c^{(0)} + c^{(1)} + c^{(2)} + t_2^{(5)}$. Then $L^{(i)}(s^{(5)}) = L(c^{(i)}), 0 \leq i \leq 2$. It is easy to verify that $k^{(3)} = 12 < W_H(c^{(0)} + c^{(1)} + c^{(2)}) = 16$. This is the case of ii).

Example 4.4.2 Let
$c^{(0)} = \{11001100\ 00000000\ 00000000\ 00000000\}$,
$c^{(1)} = \{10101010\ 10101010\ 00000000\ 00000000\}$,
$c^{(2)} = \{01100110\ 01100110\ 01100110\ 01100110\}$,
$c^{(3)} = \{10101010\ 10101010\ 10101010\ 10101010\}$,
and $s^{(5)} = c^{(0)} + c^{(1)} + c^{(2)} + c^{(3)}$. Then $L^{(i)}(s^{(5)}) = L(c^{(i)}), 0 \leq i \leq 3$. $k^{(3)} = W_H(c^{(0)} + c^{(1)} + c^{(2)}) = 12$, $k^{(4)} = W_H(c^{(0)} + c^{(1)} + c^{(2)} + c^{(3)}) = 16$. This is the case of i).

Example 4.4.3 We now still use the sequence $s^{(4)} = \{1101\ 1001\ 1000\ 0000\}$ to illustrate Theorem 4.4.1. Let
$c^{(0)} = \{0100\ 1000\ 0000\ 0000\}$,
$t_0^{(4)} = \{1001\ 0001\ 1000\ 0000\}$. Then $s^{(4)} = c^{(0)} + t_0^{(4)}$.

Let
$c^{(0)} = \{0000\ 1100\ 0000\ 0000\}$,
$c^{(1)} = \{0101\ 0101\ 0000\ 0000\}$,
$t_1^{(4)} = \{1000\ 0000\ 1000\ 0000\}$. Then $s^{(4)} = c^{(0)} + c^{(1)} + t_1^{(4)}$.

Let
$c^{(0)} = \{0000\ 0100\ 0000\ 1000\}$,
$c^{(1)} = \{0100\ 0100\ 0001\ 0001\}$,
$c^{(2)} = \{1001\ 1001\ 1001\ 1001\}$,

$t_2^{(4)} = \{0000\ 0000\ 0000\ 0000\}$. Then $s^{(4)} = c^{(0)} + c^{(1)} + c^{(2)} + t_2^{(4)}$. It is easy to verify that $k^{(3)} = W_H(s^{(4)}) = 6$.

One can see for any 2^n-periodic binary sequence $s^{(n)}$, there is $m > 0$, such that $L^{(m+1)}(s^{(n)}) = 0$. Then from part one of Theorem 4.4.1, we have that $s^{(n)} = c^{(0)} + c^{(1)} + c^{(2)} + \cdots + c^{(m)}$, where $c^{(0)}$ is a cube with linear complexity $L(s^{(n)})$, $c^{(i)}$ is a cube with $2^{W_H(S^{(i)}(s^{(n)}))}$ nonzero elements and linear complexity $L^{(i)}(s^{(n)})$, $0 < i \leq m$.

We define $s^{(n)} = c^{(0)} + c^{(1)} + c^{(2)} + \cdots + c^{(m)}$ as **the k-error cube decomposition** of a 2^n-periodic binary sequence $s^{(n)}$. For a 2^n-periodic binary sequence $s^{(n)}$, its k-error cube decomposition may be not unique and different from its standard cube decomposition, which is unique. For sequence $\{1101\ 1001\ 1000\ 0000\}$ used in standard decomposition, its k-error cube decomposition is different from its standard decomposition and is given as follows: $\{0000\ 0100\ 0000\ 1000\}$, $\{0100\ 0100\ 0001\ 0001\}$, $\{1001\ 1001\ 1001\ 1001\}$.

From part one of Theorem 4.4.1, one can see that there exists a k-error cube decomposition for a given 2^n-periodic binary sequence. Next we will use part two of Theorem 4.4.1 to find the second and third descent points.

Theorem 4.4.2 For a 2^n-periodic binary sequence $s^{(n)}$, the second descent point of the k-error linear complexity is reached by $k^{(2)} = 2^{W_H(S(s^{(n)}))} + 2^{W_H(S^{(1)}(s^{(n)}))} - 2 \times 2^{W_H(S(s^{(n)}) \cap S^{(1)}(s^{(n)}))}$.

Proof. i) First we consider the case that $L(s^{(n)}) = 2^n$. In this case, $S(s^{(n)}) = S(2^n - L(s^{(n)}))$ only contains zero elements. So, we only need prove that $k^{(2)} = 2^0 + 2^{W_H(S^{(1)}(s^{(n)}))} - 2 \times 2^0 = 2^{W_H(S^{(1)}(s^{(n)}))} - 1$.

From the part two of Theorem 4.4.1, $s^{(n)} = c^{(0)} + c^{(1)} + t^{(n)}$, where $c^{(0)}$ is a 0-cube (one nonzero element), $c^{(1)}$ is a cube with $2^{W_H(S^{(1)}(s^{(n)}))}$ nonzero elements and linear complexity $L^{(1)}(s^{(n)})$, and $L(t^{(n)}) < L^{(1)}(s^{(n)})$. $c^{(1)}$ is constructed by adding a 2^n-periodic binary sequence $c^{(0)}$ to $s^{(n)}$. We need to consider the following two cases.

In the case that $W_H(c^{(0)} + c^{(1)}) = W_H(c^{(0)}) + W_H(c^{(1)})$, from Lemma 2.1.2 in Section 2.1, $L^{(1)}(s^{(n)})$ is achieved by changing $c^{(0)}$ to a zero element, and $L^{(2)}(s^{(n)})$ is achieved by constructing another cube c_2 with linear complexity $L^{(1)}(s^{(n)})$, and using $c^{(0)}$ as a nonzero element of c_2. Thus $k^{(2)} = 2^{W_H(S^{(1)}(s^{(n)}))} - 1$.

(For example, $u^{(4)} = \{1111\ 1000\ 0000\ 0000\}$. $L^{(1)}(u^{(4)}) = 2^4 - (1 + 2)$ is achieved by a 2-

cube $\{1111\ 0000\ 0000\ 0000\}$. So $L^{(2)}(u^{(4)})$ is achieved by a 3-cube $\{1111\ 1111\ 0000\ 0000\}$, $k^{(2)} = 2^2 - 1 = 3$.)

In the case that $W_H(c^{(0)} + c^{(1)}) < W_H(c^{(0)}) + W_H(c^{(1)})$, by changing the nonzero elements of $c^{(0)} + c^{(1)}$ to zero elements, the new linear complexity $L(s^{(n)})$ will be less than $L^{(1)}(s^{(n)})$. Thus $k^{(2)} = 2^{W_H(S^{(1)}(s^{(n)}))} - 1$.

ii) Second we consider the case that $L(s^{(n)}) < 2^n$.

From the part two of Theorem 4.4.1, suppose that $s^{(n)} = c^{(0)} + c^{(1)} + t^{(n)}$, where $c^{(0)}$ is a cube with $2^{W_H(S(s^{(n)}))}$ nonzero elements and linear complexity $L(s^{(n)})$, and $c^{(1)}$ is a cube with $2^{W_H(S^{(1)}(s^{(n)}))}$ nonzero elements and linear complexity $L^{(1)}(s^{(n)})$, and $L(t^{(n)}) < L^{(1)}(s^{(n)}) < L(s^{(n)})$.

If $W_H(c^{(0)} + c^{(1)}) = W_H(c^{(0)}) + W_H(c^{(1)})$, it is obvious that by changing $2^{W_H(S(s^{(n)}))} - 2^{W_H(S(s^{(n)}) \cap S^{(1)}(s^{(n)}))} + 2^{W_H(S^{(1)}(s^{(n)}))} - 2^{W_H(S(s^{(n)}) \cap S^{(1)}(s^{(n)}))}$ nonzero elements, one can construct another cube c_2 with linear complexity $L^{(1)}(s^{(n)})$, and using $2^{W_H(S(s^{(n)}) \cap S^{(1)}(s^{(n)}))}$ nonzero elements of $c^{(0)}$. From Lemma 2.1.2 in Section 2.1, $L(c^{(1)} + c_2) < L(c^{(1)}) = L^{(1)}(s^{(n)})$. Thus the new linear complexity $L(s^{(n)})$ will be less than $L^{(1)}(s^{(n)})$.

In the case that $W_H(c^{(0)} + c^{(1)}) < W_H(c^{(0)}) + W_H(c^{(1)})$, by changing $2^{W_H(S(s^{(n)}))} - 2^{W_H(S(s^{(n)}) \cap S^{(1)}(s^{(n)}))} + 2^{W_H(S^{(1)}(s^{(n)}))} - 2^{W_H(S(s^{(n)}) \cap S^{(1)}(s^{(n)}))}$ nonzero elements, one can still construct another cube c_2 with linear complexity $L^{(1)}(s^{(n)})$, and using $2^{W_H(S(s^{(n)}) \cap S^{(1)}(s^{(n)}))}$ nonzero elements of $c^{(0)}$. Thus the new linear complexity $L(s^{(n)})$ will be less than $L^{(1)}(s^{(n)})$. In this case, c_2 may be the same as $c^{(1)}$.

So $k^{(2)} = 2^{W_H(S(s^{(n)}))} + 2^{W_H(S^{(1)}(s^{(n)}))} - 2 \times 2^{W_H(S(s^{(n)}) \cap S^{(1)}(s^{(n)}))}$.

(For example, let $c^{(0)} = \{0101\ 0000\ 0000\ 1010\}$, $c^{(1)} = \{1010\ 1010\ 1010\ 1010\}$. Then $c^{(0)} + c^{(1)} = \{1111\ 1010\ 1010\ 0000\}$, where $c^{(0)}$ and $c^{(1)}$ share 2 nonzero elements $\{1010\}$. So $k^{(2)} = 2^2 + 2^3 - 2 \times 2^1 = 8$.)

This completes the proof. □

In fact, Chang and Wang (2013) proved this result in their Theorem 3 with a much complicated approach.

Next we investigate the computation of the third descent point for the k-error linear

complexity based on the linear complexity, the first and second descent points for the k-error linear complexity. Before present our main result, we first give a result in special case.

Proposition 4.4.1 For a 2^n-periodic binary sequence $s^{(n)}$, let $k^{(i)}$ denote the ith descent point of the k-error linear complexity, $i > 0$. If $S^{(i)}(s^{(n)}) \supset S^{(0)}(s^{(n)}) \cup S^{(1)}(s^{(n)}) \cup \cdots \cup S^{(i-1)}(s^{(n)})$, then $k^{(i+1)} = 2^{W_H(S^{(i)}(s^{(n)}))} - k^{(i)}$, $i > 1$.

Proof. As $S^{(i)}(s^{(n)}) \supset S^{(0)}(s^{(n)}) \cup S^{(1)}(s^{(n)}) \cup \cdots \cup S^{(i-1)}(s^{(n)})$, by changing $2^{W_H(S^{(i)}(s^{(n)}))} - k^{(i)}$ elements of $s^{(n)}$, the linear complexity of $s^{(n)}$ becomes 0 or less than $L^{(i)}(s^{(n)})$. So $k^{(i+1)} = 2^{W_H(S^{(i)}(s^{(n)}))} - k^{(i)}$. □

For example, let $s^{(4)} = \{1111\ 1111\ 1110\ 0000\}, n = 4$. Then $S^{(0)}(s^{(n)}) = \{0000\}$, $S^{(1)}(s^{(n)}) = \{0011\}$, $S^{(2)}(s^{(n)}) = \{0111\}$, $S^{(3)}(s^{(n)}) = \{1111\}$. So $S^{(3)}(s^{(n)}) \supset S^{(0)}(s^{(n)}) \cup S^{(1)}(s^{(n)}) \cup S^{(2)}(s^{(n)})$.

As $L^{(1)}(s^{(4)})$ is achieved by a 2-cube $\{0000\ 0000\ 1111\ 0000\}$, $k^{(1)} = 1$, $L^{(2)}(s^{(4)})$ is achieved by a 3-cube $\{1111\ 1111\ 0000\ 0000\}$, $k^{(2)} = 3$. So $k^{(3)} = 2^3 - 3 = 5$. By changing $k^{(3)}$ elements, $s^{(4)}$ becomes a 4-cube $\{1111\ 1111\ 1111\ 1111\}$.

As $L^{(3)}(s^{(4)})$ is achieved by a 4-cube $\{1111\ 1111\ 1111\ 1111\}$, $k^{(3)} = 5$, thus $k^{(4)} = 2^4 - 5 = 11$. By changing $k^{(4)}$ elements, the linear complexity of $s^{(4)}$ becomes 0.

The above result is for the ith descent point computation in some special cases. Next we will investigate the third descent point in general. First, we give the the famous principle of inclusion-exclusion in combinatorics for finite sets $A_1, \cdots, A_n$, which can be stated as follows.

$$|\bigcup_{i=1}^{n} A_i| = \sum_{i=1}^{n} |A_i| - \sum_{1 \le i < j \le n} |A_i \cap A_j| + \sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k| - \cdots + (-1)^{n-1} |A_1 \cap \cdots \cap A_n|$$

Based on the principle of inclusion-exclusion, we give the following important theorem on the third descent point.

Theorem 4.4.3 For a 2^n-periodic binary sequence $s^{(n)}$, let $k^{(i)}$ denote the ith descent point of the k-error linear complexity, $i > 0$, and

$$i_{m(S1 \setminus S0S2)} = S^{-m}\{S^{(1)}(s^{(n)}) \setminus [S^{(1)}(s^{(n)}) \cap (S^{(0)}(s^{(n)}) \cup S^{(2)}(s^{(n)}))]\}.$$

With the following conditions

(i) $W_H[S^{(1)}(s^{(n)}) \cap (S^{(0)}(s^{(n)}) \cup S^{(2)}(s^{(n)}))] < W_H(S^{(1)}(s^{(n)}))$

(ii) $\{S^{(0)}(s^{(n)}) \cap S^{(2)}(s^{(n)}) = S^{(0)}(s^{(n)}) \cap S^{(1)}(s^{(n)}) \cap S^{(2)}(s^{(n)})$

(iii)

$$[i_{m(S1\setminus S0S2)} > \min\{S^{-1}(S^{(1)}(s^{(n)}) \cap S^{(2)}(s^{(n)})), S^{-1}(S^{(0)}(s^{(n)}) \cap S^{(2)}(s^{(n)}))\}$$

and

$$(S^{(0)}_{>i_{m(S1\setminus S0S2)}}(s^{(n)}) \cap S^{(2)}_{>i_{m(S1\setminus S0S2)}}(s^{(n)})) \subset S^{(1)}(s^{(n)})]\}$$

If (i) and (ii) or (i) and (iii) hold, then
$k^{(3)} = 2^{W_H(S^{(0)}(s^{(n)}))} + 2^{W_H(S^{(1)}(s^{(n)}))} + 2^{W_H(S^{(2)}(s^{(n)}))}$

$-2 \times 2^{W_H(S^{(0)}(s^{(n)}) \cap S^{(1)}(s^{(n)}))} - 2 \times 2^{W_H(S^{(0)}(s^{(n)}) \cap S^{(2)}(s^{(n)}))}$

$-2 \times 2^{W_H(S^{(1)}(s^{(n)}) \cap S^{(2)}(s^{(n)}))} + 2 \times 2^{W_H(S^{(0)}(s^{(n)}) \cap S^{(1)}(s^{(n)}) \cap S^{(2)}(s^{(n)}))}$;

Otherwise, we have
$k^{(3)} = 2^{W_H(S^{(0)}(s^{(n)}))} + 2^{W_H(S^{(1)}(s^{(n)}))} + 2^{W_H(S^{(2)}(s^{(n)}))}$

$-2 \times 2^{W_H(S^{(0)}(s^{(n)}) \cap S^{(1)}(s^{(n)}))} - 2 \times 2^{W_H(S^{(0)}(s^{(n)}) \cap S^{(2)}(s^{(n)}))}$

$-2 \times 2^{W_H(S^{(1)}(s^{(n)}) \cap S^{(2)}(s^{(n)}))} + 4 \times 2^{W_H(S^{(0)}(s^{(n)}) \cap S^{(1)}(s^{(n)}) \cap S^{(2)}(s^{(n)}))}$.

Proof. The following proof is based on the framework that $s^{(n)} = c^{(0)} + c^{(1)} + c^{(2)} + \cdots + c^{(i)} + t_i^{(n)}$. For $c^{(0)} + c^{(1)} + c^{(2)} + \cdots + c^{(i)}$, by changing $k^{(i+1)}$ elements, the linear complexity of $c^{(0)} + c^{(1)} + c^{(2)} + \cdots + c^{(i)}$ can become 0 (in which case $k^{(i+1)} = W_H(c^{(0)} + c^{(1)} + c^{(2)} + \cdots + c^{(i)})$) or less than $L(c^{(i)})$ (where $k^{(i+1)} < W_H(c^{(0)} + c^{(1)} + c^{(2)} + \cdots + c^{(i)})$).

In the case that the linear complexity of $c^{(0)} + c^{(1)} + c^{(2)} + \cdots + c^{(i)}$ becomes less than $L(c^{(i)})$, our key approach is try to construct a cube $c_1^{(i)}$, so that $L(c_1^{(i)}) = L(c^{(i)})$ and the linear complexity of $c^{(0)} + c^{(1)} + c^{(2)} + \cdots + c_1^{(i)}$ becomes 0 by changing $k^{(i+1)}$ elements, which implies that $c^{(0)} + c^{(1)} + c^{(2)} + \cdots + c_1^{(i)}$ has exactly $k^{(i+1)}$ nonzero elements.

Therefore, the computation of $k^{(i+1)}$ is equivalent to counting the nonzero elements of $c^{(0)} + c^{(1)} + c^{(2)} + \cdots + c_1^{(i)}$.

In the principle of inclusion-exclusion, if $A_1 \cap A_2$ is not empty, then $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$.

In the computation of $k^{(i+1)}$, if $W_H(S(c^{(0)}) \cap S(c^{(1)})) \neq 0$, then $c^{(0)}$ and $c^{(1)}$ can have common nonzero elements, the number of nonzero elements of $c^{(0)} + c^{(1)}$ can become $W_H(c^{(0)}) + W_H(c^{(1)}) - 2 \times 2^{W_H(S(c^{(0)}) \cap S(c^{(1)}))}$.

From Theorem 4.4.1, suppose that $s^{(n)} = c^{(0)} + c^{(1)} + c^{(2)} + t^{(n)}$, where $c^{(0)}$ is a cube with linear complexity $L(s^{(n)})$, $c^{(1)}$ is a cube with linear complexity $L^{(1)}(s^{(n)})$, $c^{(2)}$ is a cube with linear complexity $L^{(2)}(s^{(n)})$, and $L(t^{(n)}) < L^{(2)}(s^{(n)})$.

By Theorem 4.4.2, $k^{(2)} = 2^{W_H(c^{(0)})} + 2^{W_H(c^{(1)})} - 2 \times 2^{W_H(S(c^{(0)}) \cap S(c^{(1)}))}$. After changing $k^{(2)}$ nonzero elements, the sequence becomes $c^{(2)} + t^{(n)}$, where $L(t^{(n)}) < L(c^{(2)})$. Thus $W_H(c^{(0)} + c^{(1)}) = 2^{W_H(c^{(0)})} + 2^{W_H(c^{(1)})} - 2 \times 2^{W_H(S(c^{(0)}) \cap S(c^{(1)}))}$.

Without loss of generality, we consider the superposition of $c^{(0)}$ and $c^{(1)}$ with the alignment of first nonzero elements of two cubes. Then $c^{(0)} + c^{(1)}$ has exactly $k^{(2)} = 2^{W_H(c^{(0)})} + 2^{W_H(c^{(1)})} - 2 \times 2^{W_H(S(c^{(0)}) \cap S(c^{(1)}))}$ nonzero elements.

We construct a cube $c_1^{(2)}$ with linear complexity $L^{(2)}(s^{(n)})$, and furthermore, we consider the superposition of $c^{(0)}$, $c^{(1)}$ and $c_1^{(2)}$ with the alignment of first nonzero elements of three cubes. Then with an analysis similar to the principle of inclusion-exclusion, we have that $c^{(0)} + c^{(1)} + c_1^{(2)}$ has exactly $2^{W_H(S(c^{(0)}))} + 2^{W_H(S(c^{(1)}))} + 2^{W_H(S(c^{(2)}))} - 2 \times 2^{W_H(S(c^{(0)}) \cap S(c^{(1)}))} - 2 \times 2^{W_H(S(c^{(0)}) \cap S(c^{(2)}))} - 2 \times 2^{W_H(S(c^{(1)}) \cap S(c^{(2)}))} + 4 \times 2^{W_H(S(c^{(0)}) \cap S(c^{(1)}) \cap S(c^{(2)}))}$ nonzero elements.

By adding $c^{(0)} + c^{(1)} + c_1^{(2)}$ to $s^{(n)} = c^{(0)} + c^{(1)} + c^{(2)} + t^{(n)}$, we have $c_1^{(2)} + c^{(2)} + t^{(n)}$. From Lemma 2.1.2 in Section 2.1, $L(c_1^{(2)} + c^{(2)}) < L^{(2)}(s^{(n)})$. Thus $k^{(3)} \leq W_H(c^{(0)} + c^{(1)} + c_1^{(2)}) = 2^{W_H(S(c^{(0)}))} + 2^{W_H(S(c^{(1)}))} + 2^{W_H(S(c^{(2)}))} - 2 \times 2^{W_H(S(c^{(0)}) \cap S(c^{(1)}))} - 2 \times 2^{W_H(S(c^{(0)}) \cap S(c^{(2)}))} - 2 \times 2^{W_H(S(c^{(1)}) \cap S(c^{(2)}))} + 4 \times 2^{W_H(S(c^{(0)}) \cap S(c^{(1)}) \cap S(c^{(2)}))}$

(For example, let
$c^{(0)} = \{11000000\ 11000000\ 00000000\ 00000000\ 00000000\ 00000000\ 00000000\ 00000000\}$,
$c^{(1)} = \{10101010\ 00000000\ 10101010\ 00000000\ 00000000\ 00000000\ 00000000\ 00000000\}$,
$c^{(2)} = \{11110000\ 00000000\ 00000000\ 00000000\ 11110000\ 00000000\ 00000000\ 00000000\}$.

Then $c^{(0)} + c^{(1)} + c^{(2)}$ has exactly $2^{W_H(S(c^{(0)}))} + 2^{W_H(S(c^{(1)}))} + 2^{W_H(S(c^{(2)}))}$
$-2 \times 2^{W_H(S(c^{(0)}) \cap S(c^{(1)}))} - 2 \times 2^{W_H(S(c^{(0)}) \cap S(c^{(2)}))} - 2 \times 2^{W_H(S(c^{(1)}) \cap S(c^{(2)}))}$
$+4 \times 2^{W_H(S(c^{(0)}) \cap S(c^{(1)}) \cap S(c^{(2)}))} = 4 + 8 + 8 - 2 - 4 - 4 + 4 = 14$ nonzero elements.)

In the case that $W_H[S^{(1)}(s^{(n)}) \cap (S^{(0)}(s^{(n)}) \cup S^{(2)}(s^{(n)}))] < W_H(S^{(1)}(s^{(n)}))$ and $\{S^{(0)}(s^{(n)}) \cap S^{(2)}(s^{(n)}) = S^{(0)}(s^{(n)}) \cap S^{(1)}(s^{(n)}) \cap S^{(2)}(s^{(n)})$
or $[i_{m(S1 \setminus S0S2)} > \min\{S^{-1}(S^{(1)}(s^{(n)}) \cap S^{(2)}(s^{(n)})), S^{-1}(S^{(0)}(s^{(n)}) \cap S^{(2)}(s^{(n)}))\}$
and $(S^{(0)}_{>i_{m(S1 \setminus S0S2)}}(s^{(n)}) \cap S^{(2)}_{>i_{m(S1 \setminus S0S2)}}(s^{(n)})) \subset S^{(1)}(s^{(n)})]\}$, we try to construct a cube $c^{(2)}_{-1}$ with linear complexity $L(c^{(2)})$, so that $c^{(0)} + c^{(1)} + c^{(2)}_{-1}$ has less nonzero elements than $c^{(0)} + c^{(1)} + c^{(2)}$.

As $W_H[S^{(1)}(s^{(n)}) \cap (S^{(0)}(s^{(n)}) \cup S^{(2)}(s^{(n)}))] < W_H(S^{(1)}(s^{(n)}))$, there exist

$2^{W_H(S(c^{(0)}) \cap S(c^{(1)}) \cap S(c^{(2)}))}$ nonzero elements in $c^{(1)}$, so that such nonzero elements will not be canceled by addition operation with $c^{(0)}$ or $c^{(2)}$.

In the case that $\{S^{(0)}(s^{(n)}) \cap S^{(2)}(s^{(n)}) = S^{(0)}(s^{(n)}) \cap S^{(1)}(s^{(n)}) \cap S^{(2)}(s^{(n)})$ or
$[i_{m(S1 \setminus S0S2)} > \min\{S^{-1}(S^{(1)}(s^{(n)}) \cap S^{(2)}(s^{(n)})), S^{-1}(S^{(0)}(s^{(n)}) \cap S^{(2)}(s^{(n)}))\}$ and
$(S^{(0)}_{>i_{m(S1 \setminus S0S2)}}(s^{(n)}) \cap S^{(2)}_{>i_{m(S1 \setminus S0S2)}}(s^{(n)})) \subset S^{(1)}(s^{(n)})]\}$, one can move the first
$2^{W_H(S(c^{(0)}) \cap S(c^{(1)}) \cap S(c^{(2)}))}$ nonzero elements in $c^{(2)}$ to the corresponding locations in which the nonzero elements only appear in $c^{(1)}$. In this case, $2 \times 2^{W_H(S(c^{(0)}) \cap S(c^{(1)}) \cap S(c^{(2)}))}$ additional nonzero elements will be cancelled in $c^{(0)} + c^{(1)} + c^{(2)}_{-1}$, where $c^{(2)}_{-1}$ is the new cube with linear complexity $L(c^{(2)})$.

(We follow the above example, let,
$c^{(2)}_{-1} = \{01111000\ 00000000\ 00000000\ 00000000\ 01111000\ 00000000\ 00000000\ 00000000\}$.

Then $c^{(0)} + c^{(1)} + c^{(2)}_{-1}$ has $4 + 8 + 8 - 2 - 2 - 4 = 12$ nonzero elements.)

In other cases, if we move the first $2^{W_H(S(c^{(0)}) \cap S(c^{(1)}) \cap S(c^{(2)}))}$ nonzero elements in $c^{(2)}$ similarly as above, one can find that nonzero elements will not be reduced after adding operation of these three sequences.

(For example, let
$c^{(0)} = \{10100000\ 10100000\ 00000000\ 00000000\ 00000000\ 00000000\ 00000000\ 00000000\}$,
$c^{(1)} = \{11001100\ 00000000\ 11001100\ 00000000\ 00000000\ 00000000\ 00000000\ 00000000\}$,
$c^{(2)} = \{10101010\ 00000000\ 10101010\ 00000000\ 10101010\ 00000000\ 10101010\ 00000000\}$.

Then $S(c^{(0)}) = \{001010\}$, $S(c^{(1)}) = \{010101\}$,$S(c^{(2)}) = \{110110\}$.
$W_H[(S(c^{(0)}) \cap S(c^{(1)})) \cup (S(c^{(1)}) \cap S(c^{(2)}))] = 2 < W_H(S(c^{(1)})) = 3$ but
$S(c^{(0)}) \cap S(c^{(2)}) = \{000010\} \supset S(c^{(0)}) \cap S(c^{(1)}) \cap S(c^{(2)}) = \{000000\}$.

As $S(c^{(0)}) \cap S(c^{(2)}) = \{000010\}$, $S(c^{(1)}) \cap S(c^{(2)}) = \{010100\}$, $S(c^{(1)}) \setminus [S(c^{(1)}) \cap (S(c^{(0)}) \cup$

$S(c^{(2)}))] = \{000001\}$, so $S^{-m}(\{000001\}) = 1 < S^{-1}(\{000010\}) = 2 < S^{-1}(\{010100\}) = 4$.

Assume that
$c^{(2)}_{-1} = \{01010101\ 00000000\ 01010101\ 00000000\ 01010101\ 00000000\ 01010101\ 00000000\}$.
Then $c^{(0)} + c^{(1)} + c^{(2)}_{-1}$ still has $4 + 8 + 16 - 2 - 8 = 18$ nonzero elements.)

This completes the proof. □

Next we give some examples in different situations to illustrate the effectiveness of Theorem 4.4.3.

Example 4.4.4 Let
$c^{(0)} = \{10001000\ 00000000\ 00000000\ 00000000\ 00000000\ 00000000\ 00000000\ 00000000\}$,
$c^{(1)} = \{11000000\ 11000000\ 11000000\ 11000000\ 00000000\ 00000000\ 00000000\ 00000000\}$,
$c^{(2)} = \{11111111\ 00000000\ 11111111\ 00000000\ 11111111\ 00000000\ 11111111\ 00000000\}$.

Then $S(c^{(0)}) = \{000100\}$, $S(c^{(1)}) = \{011001\}$,$S(c^{(2)}) = \{110111\}$.
$W_H[(S(c^{(0)}) \cap S(c^{(1)})) \cup (S(c^{(1)}) \cap S(c^{(2)}))] = 2 < W_H(S(c^{(1)})) = 3$ and
$S(c^{(0)}) \cap S(c^{(2)}) = \{000100\} \supset S(c^{(0)}) \cap S(c^{(1)}) \cap S(c^{(2)}) = \{000000\}$.

As $S(c^{(1)}) \cap S(c^{(2)}) = \{010001\}$, $S(c^{(1)}) \setminus [S(c^{(1)}) \cap (S(c^{(0)}) \cup S(c^{(2)}))] = \{001000\}$, so
$i_{m(S1\setminus S0S2)} = S^{-m}(\{001000\}) = 8 > S^{-1}(\{010001\}) = 1$. As
$S_{>i_{m(S1\setminus S0S2)}}(c^{(0)}) \cap S_{>i_{m(S1\setminus S0S2)}}(c^{(2)}) = \{000000\}$, thus this is the case that
$[i_{m(S1\setminus S0S2)} > \min\{S^{-1}(S^{(1)}(s^{(n)}) \cap S^{(2)}(s^{(n)})), S^{-1}(S^{(0)}(s^{(n)}) \cap S^{(2)}(s^{(n)}))\}$
and $(S^{(0)}_{>i_{m(S1\setminus S0S2)}}(s^{(n)}) \cap S^{(2)}_{>i_{m(S1\setminus S0S2)}}(s^{(n)})) \subset S^{(1)}(s^{(n)})]\}$.

We move the first $2^{W_H(S(c^{(0)})\cap S(c^{(1)})\cap S(c^{(2)}))}$ nonzero elements in $c^{(2)}$ to the location below the not cancelled nonzero elements in $c^{(1)}$. Let,
$c^{(2)}_{-1} = \{01111111\ 10000000\ 01111111\ 10000000\ 01111111\ 10000000\ 01111111\ 10000000\}$.

It is obvious that $c^{(0)}+c^{(1)}+c^{(2)}_{-1}$ contains exactly $2+2^3+2^5-2\times2^0-2\times2^1-2\times2^2+2\times2^0 = 30$ nonzero elements. So $k^{(3)} = 30$.

Example 4.4.5 Let
$c^{(0)} = \{11001100\ 00000000\ 00000000\ 00000000\}$,
$c^{(1)} = \{10101010\ 10101010\ 00000000\ 00000000\}$,
$c^{(2)} = \{11001100\ 11001100\ 11001100\ 11001100\}$.

Then $S(c^{(0)}) = \{00101\}$, $S(c^{(1)}) = \{01110\}$,$S(c^{(2)}) = \{11101\}$.
$W_H[(S(c^{(0)}) \cap S(c^{(1)})) \cup (S(c^{(1)}) \cap S(c^{(2)}))] = 2 < W_H(S(c^{(1)})) = 3$ and
$S(c^{(0)}) \cap S(c^{(2)}) = \{00101\} \supset S(c^{(0)}) \cap S(c^{(1)}) \cap S(c^{(2)}) = \{00100\}$.

As $S(c^{(1)}) \cap S(c^{(2)}) = \{01100\}$, $S(c^{(1)}) \setminus [S(c^{(1)}) \cap (S(c^{(0)}) \cup S(c^{(2)}))] = \{00010\}$, so $i_{m(S1\setminus S0S2)} = S^{-m}(\{00010\}) = 2 > S^{-1}(\{00101\}) = 1$. As
$S_{>i_{m(S1\setminus S0S2)}}(c^{(0)}) \cap S_{>i_{m(S1\setminus S0S2)}}(c^{(2)}) = \{00100\} \subset S(c^{(1)})$, thus this is the case that
$[i_{m(S1\setminus S0S2)} > \min\{S^{-1}(S^{(1)}(s^{(n)}) \cap S^{(2)}(s^{(n)})), S^{-1}(S^{(0)}(s^{(n)}) \cap S^{(2)}(s^{(n)}))\}$ and
$(S^{(0)}_{>i_{m(S1\setminus S0S2)}}(s^{(n)}) \cap S^{(2)}_{>i_{m(S1\setminus S0S2)}}(s^{(n)})) \subset S^{(1)}(s^{(n)})]\}$.

We move the first $2^{W_H(S(c^{(0)})\cap S(c^{(1)})\cap S(c^{(2)}))}$ nonzero elements in $c^{(2)}$ to the location below the not cancelled nonzero elements in $c^{(1)}$. Let,
$c^{(2)}_{-1} = \{01100110\ 01100110\ 01100110\ 01100110\}$.

It is obvious that $c^{(0)} + c^{(1)} + c^{(2)}_{-1}$ contains exactly $2^2 + 2^3 + 2^4$
$-2 \times 2^1 - 2 \times 2^2 - 2 \times 2^2 + 2 \times 2^1 = 12$ nonzero elements. So $k^{(3)} = 12$.

Example 4.4.6 Let
$c^{(0)} = \{11110000\ 00000000\ 00000000\ 00000000\ 00000000\ 00000000\ 00000000\ 00000000\}$,
$c^{(1)} = \{11111111\ 11111111\ 00000000\ 00000000\ 00000000\ 00000000\ 00000000\ 00000000\}$,
$c^{(2)} = \{11111111\ 00000000\ 11111111\ 00000000\ 11111111\ 00000000\ 11111111\ 00000000\}$.

Then $S(c^{(0)}) = \{000011\}$, $S(c^{(1)}) = \{001111\}$,$S(c^{(2)}) = \{110111\}$.
$W_H[(S(c^{(0)}) \cap S(c^{(1)})) \cup (S(c^{(1)}) \cap S(c^{(2)}))] = 3 < W_H(S(c^{(1)})) = 4$ and
$S(c^{(0)}) \cap S(c^{(2)}) = S(c^{(0)}) \cap S(c^{(1)}) \cap S(c^{(2)}) = \{000011\}$.

So this is the case that $S^{(0)}(s^{(n)}) \cap S^{(2)}(s^{(n)}) = S^{(0)}(s^{(n)}) \cap S^{(1)}(s^{(n)}) \cap S^{(2)}(s^{(n)})$.

We move the first $2^{W_H(S(c^{(0)})\cap S(c^{(1)})\cap S(c^{(2)}))}$ nonzero elements in $c^{(2)}$ to the location below the not cancelled nonzero elements in $c^{(1)}$. Let,
$c^{(2)}_{-1} = \{00001111\ 11110000\ 00001111\ 11110000\ 00001111\ 11110000\ 00001111\ 11110000\}$, It is obvious that $c^{(0)}+c^{(1)}+c^{(2)}_{-1}$ contains exactly $2^2+2^4+2^5-2\times2^2-2\times2^2-2\times2^3+2\times2^2 = 28$ nonzero elements. So $k^{(3)} = 28$.

For $k^{(3)}$, it is easy to verify that Proposition 4.4.1 is the special case of Theorem 4.4.3.

We have tested all 2^n-periodic binary sequences ($n = 4, 5$) by a computer program to verify Theorem 4.4.3.

4.5 Summary

A new approach to determining the CELCS for the k-error linear complexity distribution of 2^n-periodic binary sequences was developed via the cube theory, the sieve method and the Games-Chan algorithm. The second descent point distribution of the 3-error linear complexity, the second descent point distribution of the 4-error linear complexity and the third descent point distribution of the 5-error linear complexity for 2^n-periodic binary sequences were characterized completely.

The k-error cube decomposition of 2^n-periodic binary sequences was also developed based on **the Cube Theory** of Chapter 3. As an extension of the work by Kurosawa *et al.* (2000), first we investigated the formula to determine the second descent points for the k-error linear complexity of 2^n-periodic binary sequences based on the linear complexity and the first descent points for the k-error linear complexity. Second, we studied the formula to determine the third descent points for the k-error linear complexity based on the linear complexity, the first and second descent points for the k-error linear complexity.

Let $s^{(n)}$ be a 2^n-periodic binary sequence with linear complexity less then 2^n. Suppose that c_1, c_2 and c_3 are in the standard cube decomposition of sequence $s^{(n)}$ and $L(s^{(n)}) = L(c_1)$. $L_6(s^{(n)}) < L_4(s^{(n)}) < L_2(s^{(n)}) < L(s^{(n)})$ if and only if c_1 is one 1-cube and c_2 is one 2-cube or c_1, c_2 and c_3 are three 1-cubes. Similarly, we can compute the number of 2^n-periodic binary sequences $s^{(n)}$ with given $L(s^{(n)})$, $L_2(s^{(n)})$, $L_4(s^{(n)})$ and $L_6(s^{(n)})$. Accordingly, the solution to the complete counting functions of 2^n-periodic binary sequences with the prescribed 6-error linear complexity can be obtained.

We expect that with the techniques proposed in this chapter, one can obtain other third and fourth descent point distributions of the k-error linear complexity for 2^n-periodic binary sequences. The expected value of the k-error linear complexity of 2^n-periodic binary sequences could also be investigated based on our results. We will continue this work in future due to its importance.

Chapter 5

Construction of 2^n-periodic binary sequences with prescribed k-error linear complexity profile

Let $N_{i,k}(L)$ be the number of 2^n-periodic binary sequences $s^{(n)}$ with linear complexity 2^n, the i-error linear complexity as the last descent point and the k-error linear complexity being L. In Chapter 4, we mainly focus on $N_{i,k}(L)$ of 2^n-periodic binary sequences $s^{(n)}$ with linear complexity 2^n or linear complexity less than 2^n. Usually only partial critical points of a 2^n-periodic binary sequences $s^{(n)}$ are considered. In contrast, all critical points of a 2^n-periodic binary sequences $s^{(n)}$, which are called the k-error linear complexity profile of the sequence, are considered in this chapter (Zhou *et al.*, 2016). The k-error linear complexity profile of a periodic sequence was first defined by Stamp and Martin (1993).

Based on the Games-Chan algorithm (Games and Chan, 1983) and the cube theory of Chapter 3, we investigate 2^n-periodic binary sequences $s^{(n)}$ with the given k-error linear complexity profile. We first classify 2^n-periodic binary sequences with the given k-error linear complexity profile having descent points 1, 3, 5 and 7 into totally 68 cases, and then present the counting formula of the periodic sequences for each case by constructing 2^n-periodic binary sequences with prescribed k-error linear complexity profile. In this chapter, with prescribed linear complexity and k-error linear complexity, we aim to construct all such 2^n-periodic binary sequences. This is a challenging problem with broad applications.

Our approach to constructing a 2^n-periodic binary sequence $s^{(n)}$ with the given k-error linear complexity profile is based on the reverse process of Games-Chan algorithm. First we construct a sequence consisting of multiple cubes but with a small period. Second we increase the period of these cubes and add more cubes at the same time. Finally we obtain the desired sequence. Next we will explain all these steps in detail.

The rest of this chapter is organized as follows. In Section 5.1, we mainly illustrate how to

construct the 2^n-periodic binary sequences with the given k-error linear complexity profile of $0 = L_7(s^{(n)}) < L_5(s^{(n)}) < L_3(s^{(n)}) < L_1(s^{(n)}) < 2^n$. In Section 5.2, we partially discuss how to construct the 2^n-periodic binary sequences with the given k-error linear complexity profile of $0 = L_8(s^{(n)}) < L_6(s^{(n)}) < L_4(s^{(n)}) < L_2(s^{(n)}) < L(s^{(n)}) < 2^n$.

5.1 The k-error linear complexity profile having descent points 1, 3, 5 and 7

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 3.2.1 in Section 3.2, the decomposition of $s^{(n)}$ does not include an m-cube for $m > 2$.

By Algorithm 3.2.1 in Section 3.2, $s^{(n)}$ 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 will cope with the three cases separately in the following theorems.

First 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 $L(c_2) > L(c_3) > L(c_4)$.

Theorem 5.1.1 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 3.2.1 in Section 3.2, 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

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

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

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

iii) Suppose that $L_1(s^{(n)})=2^n-(2^i+2^j), 0\le i<j<n$, $L_3(s^{(n)})=2^n-(2^p+2^q+2^r), 0\le p<q<r<n$ and $L_5(s^{(n)})=2^n-(2^x+2^y), 0\le x<y<n$. Then the number of 2^n-

periodic binary sequences $s^{(n)}$ can be given by

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

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

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

Proof. Suppose $s^{(n)}$ can be decomposed into one 0-cube c_1 and three 1-cubes c_2, c_3, c_4, where $L(c_2) > L(c_3) > L(c_4)$.

Assume that $L_1(s^{(n)})$ is achieved by a 3-cube. Based on the result by Kurosawa *et al.* (2000), 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 $k_{\min} = 2^{W_H(2^n - L(s))}$. For a 3-cube, $k_{\min} = 8$, which means that to further decrease the linear complexity of the 3-cube, we have to change 8 elements. So $L_5(s^{(n)}) = L_3(s^{(n)}) = L_1(s^{(n)})$. Therefore, we only consider the case that $L_5(s^{(n)})$ or $L_3(s^{(n)})$ is achieved by a 3-cube.

In summary, we need to cope with the following four cases separately, which correspond the four cases in the theorem.

A) All $L_5(s^{(n)}), L_3(s^{(n)})$, and $L_1(s^{(n)})$ are achieved by 2-cubes.

B) Only $L_5(s^{(n)})$ is achieved by a 3-cube.

C) Only $L_3(s^{(n)})$ is achieved by a 3-cube.

D) Both $L_5(s^{(n)})$ and $L_3(s^{(n)})$ are achieved by 3-cubes.

Now we prove these cases one by one.

i) Assume that $s^{(n)}$ can be decomposed into one 0-cube c_1, and three 1-cubes c_2, c_3, c_4. Now we will compute the number of sequences e with $W_H(e) = 7$, $L_1(e) = 2^n - (2^i + 2^j)$,

$L_3(e) = 2^n - (2^p + 2^q)$ and $L_5(e) = 2^n - (2^x + 2^y)$. As $j < q < y$, there are 15 possible cases:
$1.i < j < p < q < x < y$, $2.i < p < j < q < x < y$, $3.p < i < j < q < x < y$,
$4.i < j < p < x < q < y$, $5.i < j < x < p < q < y$, $6.i < x < j < p < q < y$,
$7.x < i < j < p < q < y$, $8.i < p < j < x < q < y$, $9.i < p < x < j < q < y$,
$10.i < x < p < j < q < y$, $11.x < i < p < j < q < y$, $12.p < i < j < x < q < y$,
$13.p < i < x < j < q < y$, $14.p < x < i < j < q < y$, $15.x < p < i < j < q < y$.

1. In the case of $i < j < p < q < x < y$.

As the number of 2^j-periodic binary sequences $e^{(j)}$ with linear complexity 2^j and $W_H(e^{(j)}) = 1$ is 2^j, thus the number of 2^{j+1}-periodic binary sequences $e^{(j+1)}$ with linear complexity $2^{j+1} - 2^j = 2^j$ and $W_H(e^{(j+1)}) = 2$ is 2^j. We use the following nine steps to construct all the required sequences.

Step 1. one nonzero element is added so that $L_1(e^{(j+1)}) = 2^{j+1} - (2^i + 2^j)$, which means that we can place a nonzero element p_3 in $e^{(j+1)}$, such that both the distance (based on Definition 2.1) of p_1 and p_3, and the distance of p_2 and p_3 are 2^i, where p_1 and p_2 are in $e^{(j+1)}$, and the distance of p_1 and p_2 is 2^j. The number of such new sequences $e^{(j+1)}$ becomes $2^j \times \frac{2^{j+1}}{2^{i+1}} = 2^{2j-i}$.

Step 2, we construct $e^{(p)}$ so that $L_1(e^{(p)}) = 2^p - (2^i + 2^j)$. The number of such $e^{(p)}$ is $2^{2j-i} \times (2^3)^{p-j-1} = 2^{3p-j-i-3}$.

Step 3, we construct $e^{(p+1)}$ by adding another nonzero element p_4 so that the distance of p_4 and one nonzero element of p_1, p_2 or p_3 is 2^p. There are 3 options. For the convenience of presentation, suppose that the distance of p_4 and p_1 is 2^p. Then p_2 and p_3 have 2^2 options. The number of such $e^{(p+1)}$ becomes $2^{3p-j-i-3} \times 3 \times 2^2$.

Step 4, we construct $e^{(q)}$ so that the distance among p_1, p_2, p_3 and p_4 are unchanged. The number of such $e^{(q)}$ becomes $2^{3p-j-i-3} \times 3 \times 2^2 \times (2^4)^{q-p-1} = 3 \times 2^{4q-p-j-i-5}$.

Step 5, we construct $e^{(q+1)}$ by adding nonzero element p_5 so that the distance of p_5 and one nonzero element of p_1, p_4 is 2^q. There are 2 options. For the convenience of presentation, suppose that the distance of p_5 and p_1 is 2^q. Then p_2, p_3 and p_4 have 2^3 options. The number of such $e^{(q+1)}$ becomes $3 \times 2^{4q-p-j-i-5} \times 2 \times 2^3 = 3 \times 2^{4q-p-j-i-1}$.

Step 6, we construct $e^{(x)}$ so that the distance among p_1, p_2, p_3, p_4 and p_5 are unchanged. The number of such $e^{(x)}$ becomes $3 \times 2^{4q-p-j-i-1} \times (2^5)^{x-q-1} = 3 \times 2^{5x-q-p-j-i-6}$.

Step 7, we construct $e^{(x+1)}$ by adding a nonzero element p_6 so that the distance of p_6 and one nonzero element of p_1, p_2, p_3, p_4 or p_5 is 2^x. There are 5 options. For the convenience of presentation, suppose that the distance of p_6 and p_1 is 2^x. Then p_2, p_3, p_4 and p_5 have 2^4 options. The number of such $e^{(x+1)}$ becomes $3 \times 2^{5x-q-p-j-i-6} \times 5 \times 2^4 = 15 \times 2^{5x-q-p-j-i-2}$.

Step 8, we construct $e^{(y)}$ so that the distance among p_1, p_2, p_3, p_4, p_5 and p_6 are unchanged. The number of such $e^{(y)}$ becomes $15 \times 2^{5x-q-p-j-i-2} \times (2^6)^{y-x-1} = 15 \times 2^{6y-x-q-p-j-i-8}$.

Step 9, construct $e^{(y+1)}$ by adding nonzero element p_7 so that the distance of p_7 and one nonzero element of p_1, p_6 is 2^y. There are 2 options. For the convenience of presentation, suppose that the distance of p_7 and p_1 is 2^y. Then p_2, p_3, p_4, p_5 and p_6 have 2^5 options. The number of such $e^{(y+1)}$ becomes $15 \times 2^{6y-x-q-p-j-i-8} \times 2 \times 2^5 = 15 \times 2^{6y-x-q-p-j-i-2}$.

We now prove that $L_1(e^{(y+1)}) = 2^{y+1} - (2^i + 2^j)$, $L_3(e^{(y+1)}) = 2^{y+1} - (2^p + 2^q)$ and $L_5(e^{(y+1)}) = 2^{y+1} - (2^x + 2^y)$. For the convenience of presentation, we only consider the case that the distance of p_4 and p_1, the distance of p_5 and p_1, the distance of p_6 and p_1 and the distance of p_7 and p_1, are 2^p, 2^q, 2^x and 2^y respectively.

By adding a nonzero element p_8, so that p_2, p_3, p_8 and p_4 form a 2-cube with linear complexity $2^{y+1} - (2^i + 2^j)$. Hence p_1, p_7 form a 1-cube with linear complexity $2^{y+1} - 2^y$, and p_5, p_6 form a 1-cube with linear complexity $2^{y+1} - 2^q$. So $L_1(e^{(y+1)}) = 2^{y+1} - (2^i + 2^j)$.

By changing p_2, p_3 to zeros, and adding a nonzero element p_9, so that p_4, p_5, p_9 and p_6 form a 2-cube with linear complexity $2^{y+1} - (2^p + 2^q)$. Hence p_1, p_7 form a 1-cube with linear complexity $2^{y+1} - 2^y$. So $L_3(e^{(y+1)}) = 2^{y+1} - (2^p + 2^q)$.

By changing p_2, p_3, p_4, p_5 to zeros, and adding a nonzero element p_{10}, so that p_1, p_6, p_7 and p_{10} form a 2-cube with linear complexity $2^{y+1} - (2^x + 2^y)$. So $L_5(e^{(y+1)}) = 2^{y+1} - (2^x + 2^y)$.

(We give the following example to illustrate the above proof, where the indexes of p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8, p_9 and p_{10} are 1,3,2,5,9,17,33,4,13 and 49 respectively.

For sequence {11101000 10000000 10000000 00000000 10000000 00000000 00000000 00000000}, $n = 6, i = 0, j = 1$, $p = 2, q = 3$, $x = 4, y = 5$. With 1 bit change, it becomes one 2-cube and two 1-cubes:
{11111000 10000000 10000000 00000000 10000000 00000000 00000000 00000000}.

With 3 bits change, it becomes one 2-cube and one 1-cube:

{10001000 10001000 10000000 00000000 10000000 00000000 00000000 00000000}.

With 5 bits change, it becomes a 2-cube:

{10000000 00000000 10000000 00000000 10000000 00000000 10000000 00000000}.)

Finally the number of sequences $e^{(n)}$ with $W_H(e^{(n)}) = 7$, $L_1(e^{(n)}) = 2^n - (2^i + 2^j)$, $L_3(e^{(n)}) = 2^n - (2^p + 2^q)$ and $L_5(e^{(n)}) = 2^n - (2^x + 2^y)$ can be given by

$$15 \times 2^{6y-x-q-p-j-i-2} \times (2^7)^{n-y-1} = 15 \times 2^{7n-y-x-q-p-j-i-9}.$$

2. In the case of $i < p < j < q < x < y$. One 1-cube with linear complexity $2^{q+1} - 2^q$ is added so that $L_3(e^{(q+1)}) = 2^{q+1} - (2^p + 2^q)$. Suppose that there are nonzero elements p_1, p_2, p_3, p_4 and p_5 in $e^{(q+1)}$. The distance of p_1 and p_2 are 2^i, p_2 and p_3 are 2^p, p_1 and p_4 are 2^j, p_2 and p_5 are 2^q or p_3 and p_5 are 2^q. Note that the distance of p_1 and p_3 are 2^i, thus the number of $e^{(q+1)}$ of this kind is $2^{2j-i} \times 2^{j-p} \times (2^4)^{q-j-1} \times 2^3$.

Assume that The distance of p_1 and p_2 are 2^i, p_1 and p_3 are 2^p, p_1 and p_4 are 2^j, p_3 and p_5 are 2^q. Thus the number of this kind $e^{(q+1)}$ is $2^{2j-i} \times 2^{j-p} \times (2^4)^{q-j-1} \times 2^3$.

So, the number of $e^{(q+1)}$ becomes $2^{2j-i} \times 2 \times 2^{j-p} \times (2^4)^{q-j-1} \times 2^3 = 2 \times 2^{4q-p-j-i-1}$. Similarly, the number of sequences $e^{(n)}$ can be given by

$$2 \times 5 \times 2^{6y-x-q-p-j-i-2} \times (2^7)^{n-y-1} = 2 \times 5 \times 2^{7n-y-x-q-p-j-i-9}.$$

3. In the case of $p < i < j < q < x < y$. One 1-cube with linear complexity $2^{q+1} - 2^q$ is added so that $L_3(e^{(q+1)}) = 2^{q+1} - (2^p + 2^q)$. The number of $e^{(q+1)}$ becomes $2^{2j-i} \times 2^{j-p} \times (2^4)^{q-j-1} \times 2^3 = 2^{4q-p-j-i-1}$.

The number of sequences $e^{(n)}$ can be given by

$$5 \times 2^{6y-x-q-p-j-i-2} \times (2^7)^{n-y-1} = 5 \times 2^{7n-y-x-q-p-j-i-9}.$$

4. In the case of $i < j < p < x < q < y$. One 1-cube with linear complexity $2^{y+1} - 2^y$ is added so that $L_5(e^{(y+1)}) = 2^{y+1} - (2^x + 2^y)$. The number of $e^{(y+1)}$ becomes $3 \times 2^{4q-p-j-i-1} \times 4 \times 2^{q-x} \times (2^6)^{y-q-1} \times 2^5 = 3 \times 4 \times 2^{6y-x-q-p-j-i-2}$.

The number of sequences $e^{(n)}$ can be given by

$$3 \times 4 \times 2^{6y-x-q-p-j-i-2} \times (2^7)^{n-y-1} = 3 \times 4 \times 2^{7n-y-x-q-p-j-i-9}.$$

5. In the case of $i < j < x < p < q < y$. One 1-cube with linear complexity $2^{y+1} - 2^y$ is added so that $L_5(e^{(y+1)}) = 2^{y+1} - (2^x + 2^y)$. The number of $e^{(y+1)}$ becomes $3 \times 2^{4q-p-j-i-1} \times 3 \times 2^{q-x} \times (2^6)^{y-q-1} \times 2^5 = 3^2 \times 2^{6y-x-q-p-j-i-2}$.

The number of sequences $e^{(n)}$ can be given by

$$3^2 \times 2^{6y-x-q-p-j-i-2} \times (2^7)^{n-y-1} = 3^2 \times 2^{7n-y-x-q-p-j-i-9}.$$

The other 10 cases can obtained similarly. Based on the above results, the numbers of sequences $e^{(n)}$ can be given as follows.

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

ii) Assume that $s^{(n)}$ can be decomposed into one 0-cube c_1, and three 1-cubes c_2, c_3, c_4, where $L(c_2) > L(c_3) > L(c_4)$, $L_1(s^{(n)}) = 2^n - (2^i + 2^j), 0 \le i < j < n$, $L_3(s^{(n)}) = 2^n - (2^p + 2^q), 0 \le p < q < n$ and $L_5(s^{(n)}) = 2^n - (2^x + 2^y + 2^z), 0 \le x < y < z < n$. It is easy to prove that $L(c_2) = 2^n - 2^j$, $L(c_3) = 2^n - 2^q$ and $L(c_4) = 2^n - 2^z$ (refer to Appendix 6) for the proof).

Note that by Algorithm 3.2.1 in Section 3.2, we have a standard cube decomposition, but $s^{(n)}$ may have other cube decompositions.

As $L_5(s^{(n)}) = 2^n - (2^x + 2^y + 2^z)$, thus $L_5(s^{(n)})$ is achieved by a 3-cube $\ddot{c}$. If $\ddot{c}$ includes 7 nonzero elements of $s^{(n)}$, then $L_5(s^{(n)}) = L_1(s^{(n)})$, which is a contradiction. If $\ddot{c}$ includes

6 nonzero elements of $s^{(n)}$, then $L_5(s^{(n)}) = L_3(s^{(n)})$, which is a also contradiction. So $\ddot{c}$ should only include 5 nonzero elements of $s^{(n)}$.

Thus $s^{(n)}$ include a 2-cube (refer to Appendix 4) for the proof).

(For example, Sequence {11100000 10001000 10001000 00000000}, $n = 5$, can be decomposed into one 0-cube c_1, and three 1-cubes c_2, c_3, c_4. At the same time, the sequence includes a 2-cube {00000000 10001000 10001000 00000000}.)

Suppose that the 0-cube c_1 includes a nonzero element e_1, the 1-cubes c_2 and c_3 includes 4 nonzero elements e_2, e_3, e_4, e_5, and the 1-cube c_4 includes 2 nonzero elements e_6, e_7. Thus $\ddot{c}$ should include e_6, e_7.

If $L(c_3) = 2^n - 2^q$, then $L_3(s^{(n)}) = 2^n - (2^p + 2^q)$.

According to Appendix 4), we may assume that e_1, e_2, e_3 and e_7 constitute a 2-cube with linear complexity $2^n - (2^x + 2^y)$.

When we implement Step 2 of Algorithm 3.1.1 in Section 3.1, if the nonzero elements are canceled in the second time, we assume the removed two nonzero elements are e_2, e_3, then this is the case that $q = y$. So $j < q = y$. As e_1, e_2, e_3 and e_7 constitute a 2-cube with linear complexity $2^n - (2^x + 2^y)$, thus $p \geq x$, $D(e_1, e_2) = 2^x$, $D(e_1, e_7) = 2^y$. If $p = x$, the possible cases are:

$i < j < p = x < q = y < z$,

$i < p = x < j < q = y < z$,

$p = x < i < j < q = y < z$.

If $p > x$, then without loss of generality we suppose that $D(e_2, e_4) = 2^p$, so $D(e_1, e_4) \equiv D(e_1, e_2) + D(e_2, e_4) \mod (2^p) = 2^x$. As $2^n - (2^i + 2^j)$ is determined by the distance among e_1, e_4, e_5, so $x = i$ or j. The possible cases are:

$i < j = x < p < q = y < z$,

$i = x < j < p < q = y < z$,

$i = x < p < j < q = y < z$.

When we implement Step 2 of Algorithm 3.1.1 in Section 3.1, if the nonzero elements are canceled in the second time, we assume the two nonzero elements are e_4, e_5, then this is the case that $i = x, j = y < q$, but $p \neq x, p \neq y$ (refer to Appendix 5) for the proof)

The possible cases are:

$i = x < j = y < p < q < z$,

$i = x < p < j = y < q < z$,

$p < i = x < j = y < q < z$.

When we implement Step 2 of Algorithm 3.1.1 in Section 3.1, if the nonzero elements are canceled in the second time, we assume the removed two nonzero elements are e_3, e_4, then we only need to consider 3 cases as below:

$i = x < j < p = y < q$,

$i < j = x < p = y < q$,

$i < p = x < j = y < q$.

Other cases are included in previous consideration as illustrated by Appendix 7).

Now consider the case of $i < j < p = x < q = y < z$.

Suppose that $e^{(j)}$ is a 2^j-periodic binary sequence with linear complexity 2^j and $W_H(e^{(j)}) = 1$. Then the number of these $e^{(j)}$ is 2^j. So the number of 2^{j+1}-periodic binary sequences $e^{(j+1)}$ with linear complexity $2^{j+1} - 2^j = 2^j$ and $W_H(e^{(j+1)}) = 2$ is also 2^j. Similarly we have the following steps to construct the required sequences.

Step 1 one nonzero element is added so that $L_1(e^{(j+1)}) = 2^{j+1} - (2^i + 2^j)$, which means that we place a nonzero element p_3 in $e^{(j+1)}$, such that both the distance of p_1 and p_3, and the distance of p_2 and p_3 are 2^i, where p_1 and p_2 are in $e^{(j+1)}$, and the distance of p_1 and p_2 is 2^j. The number of new $e^{(j+1)}$ becomes $2^j \times \frac{2^{j+1}}{2^{i+1}} = 2^j \times 2^{j-i} = 2^{2j-i}$.

Step 2 we construct $e^{(x)}$ such that $L_1(e^{(x)}) = 2^x - (2^i + 2^j)$. The number of such $e^{(x)}$ becomes $2^{2j-i} \times (2^3)^{x-j-1} = 2^{3x-j-i-3}$.

Step 3 we construct $e^{(x+1)}$ by adding another nonzero element p_4 so that the distance of p_4 and one nonzero element of p_1, p_2 or p_3 is 2^x. There are 3 options. For the convenience of presentation, suppose that the distance of p_4 and p_1 is 2^x. Then p_2 and p_3 have 2^2 options. The number of $e^{(x+1)}$ becomes $2^{3x-j-i-3} \times 3 \times 2^2$.

Step 4 we construct $e^{(y)}$ so that the distance (based on Definition 2.1) among p_1, p_2, p_3 and p_4 are unchanged. The number of $e^{(y)}$ becomes $2^{3x-j-i-3} \times 3 \times 2^2 \times (2^4)^{y-x-1} = 3 \times 2^{4y-x-j-i-5}$.

Step 5 we construct $e^{(y+1)}$ by adding two nonzero elements p_5, p_6 so that the distance of p_1 and p_5 is 2^y, and the distance of p_4 and p_6 is 2^y. The number of $e^{(y+1)}$ becomes $3 \times 2^{4y-x-j-i-5} \times 2^2$.

Step 6 we construct $e^{(z+1)}$ by adding another nonzero element p_7 so that the distance of p_7 and one nonzero element of p_1, p_5 or p_4, p_6 is 2^z. The number of $e^{(z+1)}$ becomes $3 \times 2^{4y-x-j-i-5} \times 2^2 \times 4 \times (2^5)^{z-y} = 3 \times 2^{5z-y-x-j-i-1}$.

Finally the number of sequences $e^{(n)}$ with $W_H(e^{(n)}) = 7$, $L_1(e^{(n)}) = 2^n - (2^i + 2^j)$, $L_3(e^{(n)}) = 2^n - (2^p + 2^q)$ and $L_5(e^{(n)}) = 2^n - (2^x + 2^y + 2^z)$ can be given by

$$3 \times 2^{5z-y-x-j-i-1} \times (2^7)^{n-z-1} = 3 \times 2^{7n-2z-y-x-j-i-8}.$$

(We just give the following example to illustrate the proof.

For sequence {11100000 00000000 10001000 10001000}, $n = 5, i = 0, j = 1$, $p = x = 2, q = y = 3$, $z = 4$. With 1 bit change, it becomes one 2-cube and one 2-cube: {11110000 00000000 10001000 10001000}. With 3 bits change, it becomes one 2-cube: {00000000 00000000 10001000 10001000} With 5 bits change, it becomes a 3-cube: {10001000 10001000 10001000 10001000})

For the case of $i < p = x < j < q = y < z$, here we only give the brief construction process as follows.

$e^{(j+1)} : 2^{2j-i} \times 2^{j-x} \Longrightarrow e^{(y)} : 2^{2j-i} \times 2^{j-x} \times (2^4)^{y-j-1}$

$\Longrightarrow e^{(y+1)} : 2^{2j-i} \times 2^{j-x} \times (2^4)^{y-j-1} \times 3 \times 2^2 = 3 \times 2^{4y-j-x-i-2}$

$\Longrightarrow e^{(z+1)} : 3 \times 2^{4y-j-x-i-2} \times 2 \times (2^5)^{z-y} = 3 \times 2^{5z-y-x-j-i-1}$.

For the case of $i < j = x < p < q = y < z$, the brief construction process is as follows.

$e^{(p)} : 2^{2j-i} \times (2^3)^{p-j-1} \Longrightarrow e^{(p+1)} : 2^{3p-j-i-3} \times 2 \times 2^2$

$\Longrightarrow e^{(q)} : 2^{3p-j-i} \times (2^4)^{q-p-1} \Longrightarrow e^{(q+1)} : 2^{4q-p-j-i-4} \times 2 \times 2^2$

$\Longrightarrow e^{(z)} : 2^{4q-p-j-i-1} \times (2^6)^{z-q-1} \Longrightarrow e^{(z+1)} : 2^{6z-2q-p-j-i-7} \times 2 \times 2^5 = 2^{6z-2q-p-j-i-1}$.

For the case of $i = x < j < p < q = y < z$, the brief construction process is as follows.

$e^{(y+1)} : 2^{2y-x-2} \times 2 \times 2^{y-j} \times 2 \times 2^{y-p} \Longrightarrow e^{(z)} : 2^{4y-x-j-p} \times (2^6)^{z-y-1}$

$\Longrightarrow e^{(z+1)} : 2^{6z-2y-x-p-j-6} \times 2 \times 2^5 = 2^{6z-2y-x-p-j}$.

For the case of $i = x < p < j < q = y < z$, here we only give the brief construction process as follows.

$e^{(j+1)} : 2^{2j-i} \times 2 \times 2^{j-p} \Longrightarrow e^{(q)} : 2^{3j-p-i+1} \times (2^4)^{q-j-1}$

Suppose that both the distance of p_1 and p_3, and the distance of p_2 and p_3 are 2^i, where p_1 and p_2 are in $e^{(j+1)}$, and the distance of p_1 and p_2 is 2^j. Then p_4 has 2 options: the distance of p_1 and p_4 is 2^p or the distance of p_3 and p_4 is 2^p.

Add p_5, so that the distance of p_5 and p_4 is 2^q. If the distance of p_1 and p_4 is 2^p, add p_6, so that the distance of p_6 and p_3 is 2^q; otherwise if the distance of p_3 and p_4 is 2^p, add p_6, so that the distance of p_6 and p_1 or p_2 is 2^q. There are totally 3 options.

$e^{(q+1)} : 2^{4q-p-j-i-3} \times \frac{3}{2} \times 2^2 \Longrightarrow e^{(z)} : 3 \times 2^{4q-p-j-i-2} \times (2^6)^{z-q-1} = 3 \times 2^{6z-2q-p-j-i-8}$

$\Longrightarrow e^{(z+1)} : 3 \times 2^{6z-2q-p-j-i-8} \times 2 \times 2^5 = 3 \times 2^{6z-2q-p-j-i-2}$.

For the case of $i = x < j = y < p < q < z$, here we only give the brief construction process as follows.

$e^{(p)} : 2^{2j-i-2} \times (2^4)^{p-j-1} \Longrightarrow e^{(p+1)} : 2^{4p-2j-i-6} \times 4 \times 2^3$

$\Longrightarrow e^{(q)} : 2^{4p-2j-i-1} \times (2^5)^{q-p-1} \Longrightarrow e^{(q+1)} : 2^{4p-2j-i-1} \times (2^5)^{q-p-1} \times 2 \times 2^4 = 2^{5q-p-2j-i-1}$

$\Longrightarrow e^{(z)} : 2^{5q-p-2j-i-1} \times (2^6)^{z-q-1} \Longrightarrow e^{(z+1)} : 2^{5q-p-2j-i-1} \times (2^6)^{z-q-1} \times 3 \times 2^5 = 3 \times 2^{6z-q-p-2j-i-2}$.

For the case of $i = x < p < j = y < q < z$, here we only give the brief construction process as follows.

$e^{(q)} : 2^{2j-i-2} \times 2 \times 2^{j-p} \times (2^5)^{q-j-1} \Longrightarrow e^{(q+1)} : 2^{5q-p-2j-i-6} \times 2^4$

$\Longrightarrow e^{(z)} : 2^{5q-p-2j-i-2} \times (2^6)^{z-q-1} \Longrightarrow e^{(z+1)} : 2^{6z-q-p-2j-i-8} \times (4+2) \times 2^5 = 3 \times 2^{6z-q-p-2j-i-2}$.

(The reason to multiply $1 \times 4 + 2 \times 1 = 6$ is similar to the case of $i = x < p < j < q = y < z$).

For the case of $p < i = x < j = y < q < z$, here we only give the brief construction process as follows.

$e^{(q)} : 2^{2j-i-2} \times 2^{j-p} \times (2^5)^{q-j-1} \Longrightarrow e^{(q+1)} : 2^{5q-p-2j-i-7} \times 2^4$

$\Longrightarrow e^{(z)} : 2^{5q-p-2j-i-3} \times (2^6)^{z-q-1} \Longrightarrow e^{(z+1)} : 2^{6z-q-p-2j-i-9} \times 4 \times 2^5 = 2^{6z-q-p-2j-i-2}$.

For the case of $i = x < j < p = y < q < z$, here we only give the brief construction process as follows.

$e^{(q)} : 2^{2y-i-2} \times 2 \times 2^{y-j} \times (2^5)^{q-y-1} \Longrightarrow e^{(q+1)} : 2^{5q-2y-j-i-6} \times 4 \times 2^4$

$\Longrightarrow e^{(z)} : 2^{5q-2y-j-i} \times (2^6)^{z-q-1} \Longrightarrow e^{(z+1)} : 2^{6z-q-2y-j-i-6} \times 2 \times 2^5 = 2^{6z-q-2y-j-i}$.

For the case of $i < j = x < p = y < q < z$, here we give the brief construction process as follows.

$e^{(q)} : 2^{2y-j-2} \times 2^{y-i} \times (2^5)^{q-y-1} \Longrightarrow e^{(q+1)} : 2^{5q-2y-j-i-7} \times 4 \times 2^4$

$\Longrightarrow e^{(z)} : 2^{5q-2y-j-i-1} \times (2^6)^{z-q-1} \Longrightarrow e^{(z+1)} : 2^{6z-q-2y-j-i-7} \times 2 \times 2^5 = 2^{6z-q-2y-j-i-1}$.

For the case of $i < p = x < j = y < q < z$, here we give the brief construction process as follows.

$e^{(q)} : 2^{2y-x-2} \times 2^{y-i} \times (2^5)^{q-y-1} \Longrightarrow e^{(q+1)} : 2^{5q-2y-x-i-7} \times 4 \times 2^4$

$\Longrightarrow e^{(z)} : 2^{5q-2y-x-i-1} \times (2^6)^{z-q-1} \Longrightarrow e^{(z+1)} : 2^{6z-q-2y-x-i-7} \times 2^5 = 2^{6z-q-2y-x-i-2}$.

In summary, the numbers of sequences $e^{(n)}$ can be given by

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

iii) Now we 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, $L_1(s^{(n)}) = 2^n - (2^i + 2^j), 0 \leq i < j < n$, $L_3(s^{(n)}) = 2^n - (2^p + 2^q + 2^r), 0 \leq p < q < r < n$ and $L_5(s^{(n)}) = 2^n - (2^x + 2^y), 0 \leq x < y < n$.

Suppose that the 0-cube c_1 includes a nonzero element e_1, the 1-cube c_2 includes 2 nonzero elements e_2, e_3, the 1-cube c_3 includes 2 nonzero elements e_4, e_5, and the 1-cube c_4 includes 2 nonzero elements e_6, e_7.

As c_2, c_3, c_4 are three 1-cubes and $L(c_2) > L(c_3) > L(c_4)$, so $j < r < y$.

If $L_3(s^{(n)})$ is achieved with a 3-cube $\dot{c}$ by changing e_6 or e_7, and adding two nonzero elements, then this is the case iv).

So $L_3(s^{(n)})$ is achieved with a 3-cube $\dot{c}$ composed of e_1, e_2, e_3, e_4, e_5 and three nonzero elements. Thus $\dot{c}$ contains e_1, e_2 and e_3. So $\{i, j\} \subset \{p, q, r\}$. By $j < r$, we know that $i = p, j = q$. Therefore, there are 4 cases: $i = p < j = q < r < x < y$, $i = p < j = q < x < r < y$, $i = p < x < j = q < r < y$, $x < i = p < j = q < r < y$.

1. Now consider the case of $i = p < j = q < r < x < y$.

Step 1 we construct $e^{(j+1)}$ with linear complexity $2^{j+1} - (2^i + 2^j)$.

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

For $j > i$, if 2^j-periodic binary sequences $e^{(j)}$ with linear complexity $2^j - 2^i$ and $W_H(e^{(j)}) = 2$, then $2^j - 2^i - (2^{i+1} - 2^i) = 2^{j-1} + 2^{j-2} + \cdots + 2^{i+1}$. Based on Algorithm 3.1.1 in Section 3.1, the number of these $e^{(j)}$ 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}.

Step 2 we construct $e^{(r)}$ so that the distance (based on Definition 2.1) among all nonzero elements p_1, p_2, p_3 or p_4 are unchanged. The number of $e^{(r)}$ becomes $2^{2j-i-2} \times (2^4)^{r-j-1} = 2^{4r-2j-i-6}$.

Step 3 we construct $e^{(r+1)}$ by adding one nonzero element p_5 so that the distance of p_5 and one nonzero element of p_1, p_2, p_3 or p_4 is 2^r. There are 4 options. For the convenience of presentation, suppose that the distance of p_5 and p_1 is 2^r. Then p_2, p_3 and p_4 have 2^3 options. The number of $e^{(r+1)}$ becomes $2^{4r-2j-i-6} \times 4 \times 2^3 = 2^{4r-2j-i-1}$.

Step 4 we construct $e^{(x)}$ so that the distance among all nonzero elements are unchanged. The number of $e^{(x)}$ becomes $2^{4r-2j-i-1} \times (2^5)^{x-r-1} = 2^{5x-r-2j-i-6}$.

Step 5 we construct $e^{(x+1)}$ by adding another nonzero element p_6 so that the distance of p_6 and one nonzero element of p_1, p_2, p_3 or p_4 is 2^x. There are 5 options. For the convenience of presentation, suppose that the distance of p_6 and p_1 is 2^x. Then p_2, p_3, p_4 and p_5 have 2^4 options. The number of $e^{(x+1)}$ becomes $2^{5x-r-2j-i-6} \times 5 \times 2^4 = 5 \times 2^{5x-r-2j-i-2}$.

Step 6 we construct $e^{(y)}$ so that the distance among all nonzero elements are unchanged. The number of $e^{(y)}$ becomes $2^{5x-r-2j-i-2} \times (2^6)^{y-x-1} = 2^{6y-x-r-2j-i-8}$.

Step 7 we construct $e^{(y+1)}$ by adding another nonzero element p_7 so that the distance of p_7 and one nonzero element of p_1 or p_6 is 2^y. There are 2 options. For the convenience of presentation, suppose that the distance of p_7 and p_1 is 2^x. Then p_2, p_3, p_4, p_5 and p_6 have 2^5 options. The number of $e^{(x+1)}$ becomes $2^{6y-x-r-2j-i-8} \times 2 \times 2^5 = 5 \times 2^{6y-x-r-2j-i-2}$.

Finally the number of sequences $e^{(n)}$ with $W_H(e^{(n)}) = 7$, $L_1(e^{(n)}) = 2^n - (2^i + 2^j)$, $L_3(e^{(n)}) = 2^n - (2^p + 2^q + 2^r)$ and $L_5(e^{(n)}) = 2^n - (2^x + 2^y)$ can be given by

$$5 \times 2^{6y-x-r-2j-i-2} \times (2^7)^{n-y-1} = 5 \times 2^{7n-y-x-r-2j-i-9}.$$

(For sequence {10001000 10000000 11110000 00000000}, $n = 5, i = p = 0, j = q = 1$, $r = 2, x = 3, y = 4$. With 1 bit change, it becomes one 2-cube and one 1-cube: {10000000 10000000 11110000 00000000} With 3 bits change, it becomes one 3-cube and one 1-cube: {10001111 10000000 11110000 00000000} With 5 bits change, it becomes a 2-cube: {10000000 10000000 10000000 10000000})

2. In the case of $i = p, j = q, q < x < r$. Similar to case 1, the number of $e^{(r+1)}$ in Step 1 is $2^{4r-2j-i-1}$.

In Step 2, one 1-cube with linear complexity $2^{y+1} - 2^y$ is added so that $L_5(e^{(y+1)}) = 2^{y+1} - (2^x + 2^y)$. Note that $j < x < r$, the number of $e^{(y+1)}$ becomes $2^{4r-2j-i-1} \times 2^{r-x} \times 4 \times (2^6)^{y-r-1} \times 2^5 = 2^{6y-x-r-2j-i}$.

Finally the number of sequences can be given by

$$2^{6y-x-r-2j-i} \times (2^7)^{n-y-1} = 2^{7n-y-x-r-2j-i-7}.$$

(For example, with s sequence {00000000 00000001 00000010 00011111}, $n = 5, i = 0, j = 1$, $p = 0, q = 1, r = 3$, $x = 2, y = 4$. With 1 bit change, it becomes a 2-cube and a 1-cube: {00000000 00000001 00000000 00011111}. With 3 bits change, it becomes a 3-cube and a 1-cube: {00000000 00000001 00011110 00011111}. With 5 bits change, it becomes a 2-cube: {00000000 00010001 00000000 00010001}.)

3. In the case of $i = p, j = q, p < x < q$. Similar to case 1, one 1-cube with linear complexity $2^{y+1} - 2^y$ is added so that $L_5(e^{(y+1)}) = 2^{y+1} - (2^x + 2^y)$. Note that $i < x < j$, the number of $e^{(y+1)}$ becomes $2^{4r-2j-i-1} \times 2^{r-x} \times 2 \times (2^6)^{y-r-1} \times 2^5 = 2^{6y-x-r-2j-i-1}$.

Finally the number of sequences can be given by

$$2^{6y-x-r-2j-i-1} \times (2^7)^{n-y-1} = 2^{7n-y-x-r-2j-i-8}.$$

(For sequence {00000000 00000001 00000010 01100111}, $n = 5, i = 0, j = 2$, $p = 0, q = 2, r = 3$, $x = 1, y = 4$. With 1 bit change, it becomes a 2-cube and a 1-cube: {00000000 00000001 00000000 01100111}. With 3 bits change, it becomes a 3-cube and a 1-cube: {00000000 00000001 01100110 01100111}. With 5 bits change, it becomes a 2-cube: {00000000 00000101 00000000 00000101}.)

Similarly, the numbers of sequences $e^{(n)}$ can be given by

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

iv) Finally we 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, $L_1(s^{(n)}) = 2^n - (2^i + 2^j), 0 \leq i < j < n$, $L_3(s^{(n)}) = 2^n - (2^p + 2^q + 2^r), 0 \leq p < q < r < n$ and $L_5(s^{(n)}) = 2^n - (2^x + 2^y + 2^z), 0 \leq x < y < n$. Suppose that the 0-cube c_1 includes a nonzero element e_1, the 1-cube c_2 includes 2 nonzero elements e_2, e_3, the 1-cube c_3 includes 2 nonzero elements e_4, e_5, and the 1-cube c_4 includes 2 nonzero elements e_6, e_7.

As c_2, c_3, c_4 are three 1-cubes and $L(c_2) > L(c_3) > L(c_4)$, so $j < r < z$.

Note that $L_3(s^{(n)})$ is achieved with a 3-cube $\dot{c}$ by changing e_6 or e_7, and adding two nonzero elements, thus $\dot{c}$ contains e_1, e_2 and e_3. So $\{i, j\} \subset \{p, q, r\}$. By $j < r$, we know that $i = p, j = q$.

Also, e_1, e_2, e_3, e_4, e_5 and e_6 include a 2-cube with linear complexity $2^n - (2^x + 2^y)$ (refer to Appendix 4) on the proof). Thus $\{x, y\} \subset \{p, q, r\}$. So, there are three possible cases: $i = p < j = q = x < r = y < z$, $i = p = x < j = q < r = y < z$, $i = p = x < j = q = y < r < z$.

Note that $y = r$ (refer to Appendix 8) for the proof), thus the case that $i = p = x < j = q = y < r < z$ is impossible.

Now consider the case of $i = p < j = q = x < r = y < z$ with the following steps.

Step 1 we construct $e^{(j+1)}$ with linear complexity $2^{j+1} - (2^i + 2^j)$.

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 3.1.1 in Section 3.1, 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}.

Step 2 we construct $e^{(r)}$ so that the distance (based on Definition 2.1) among all nonzero elements p_1, p_2, p_3 or p_4 are unchanged. The number of $e^{(r)}$ becomes $2^{2j-i-2} \times (2^4)^{r-j-1} = 2^{4r-2j-i-6}$.

Step 3 we construct $e^{(r+1)}$ by adding two nonzero elements p_5, p_6 so that p_5, p_6 and two nonzero elements of p_1, p_2, p_3 or p_4 constitute a 2-cube with linear complexity $2^{r+1} - (2^r + 2^j)$. There are 2 options. For the convenience of presentation, suppose that p_1, p_2, p_5 or p_6 constitute a 2-cube. Then p_3, p_4 have 2^2 options. The number of $e^{(r+1)}$ becomes $2^{4r-2j-i-6} \times 2 \times 2^2 = 2^{4r-2j-i-3}$.

Step 4 we construct $e^{(z)}$ so that the distance among all nonzero elements are unchanged. The number of $e^{(z)}$ becomes $2^{4r-2j-i-3} \times (2^6)^{z-r-1} = 2^{6z-2r-2j-i-9}$.

Step 5 we construct $e^{(z+1)}$ by adding one nonzero element p_7 so that the distance of p_7 and one nonzero elements of p_1, p_2, p_5 or p_6 is 2^z. There are 4 options. For the convenience of presentation, suppose that the distance of p_1 and p_7 is 2^z.. Then p_2, p_3, p_4, p_5 and p_6 have 2^5 options. The number of $e^{(z+1)}$ becomes $2^{6z-2r-2j-i-9} \times 4 \times 2^5 = 2^{6z-2r-2j-i-2}$.

Finally the number of sequences $e^{(n)}$ with $W_H(e^{(n)}) = 7$, $L_1(e^{(n)}) = 2^n - (2^i + 2^j)$, $L_3(e^{(n)}) = 2^n - (2^p + 2^q + 2^r)$ and $L_5(e^{(n)}) = 2^n - (2^x + 2^y + 2^z)$ can be given by

$$2^{6z-2r-2j-i-2} \times (2^7)^{n-z-1} = 2^{7n-z-2r-2j-i-9}.$$

(For sequence {11110000 10100000 10000000 00000000}, $n = 5, i = p = 0, j = q = x = 1$, $r = y = 3, z = 4$. With 1 bit change, it becomes one 2-cube and one 1-cube: {11110000 10000000 10000000 00000000} With 3 bits change, it becomes one 3-cube: {11110000 11110000 0000000 00000000} With 5 bits change, it becomes a 3-cube: {10100000 10100000 10100000 10100000})

For the case of $i = p = x < j = q < r = y < z$, here we only give the brief construction process as follows.

$e^{(r)} : 2^{2j-i-2} \times (2^4)^{r-j-1} \Longrightarrow e^{(r+1)} : 2^{4r-2j-i-6} \times 4 \times 2^2$

$\Longrightarrow e^{(z)} : 2^{4r-2j-i-2} \times (2^6)^{z-r-1} \Longrightarrow e^{(z+1)} : 2^{6z-2r-2j-i-8} \times 4 \times 2^5 = 2^{6z-2r-2j-i-1}$.

Based on the above results, the numbers of sequences $e^{(n)}$ can be given by

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

□

Now we consider the second case that $s^{(n)}$ can be decomposed into one 0-cube c_1 one 2-cube c_2 and one 1-cube c_3, where $L(c_2) > L(c_3)$.

Theorem 5.1.2 Let $s^{(n)}$ be a 2^n-periodic binary sequence with linear complexity 2^n and $L_7(s^{(n)}) = 0 < L_5(s^{(n)}) < L_3(s^{(n)}) < L_1(s^{(n)})$, and $s^{(n)}$ can be decomposed into one 0-cube c_1, one 2-cube c_2 and one 1-cube c_3, where $L(c_2) > L(c_3)$. In this case, we have two situations.

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

$$\begin{cases} 5 \times 2^{7n-y-x-q-2j-i-9}, & i=p<q<j=r<x \\ 3 \times 2^{7n-y-x-q-2j-i-9}, & i=p<q<x<j=r \\ 2^{7n-y-x-q-2j-i-8}, & i=p<x<q<j=r \\ 2^{7n-y-x-q-2j-i-9}, & x<i=p<j=r \\ 5 \times 2^{7n-y-x-p-2j-i-10}, & i=q<j=r<x \\ 3 \times 2^{7n-y-x-p-2j-i-10}, & i=q<x<j=r \\ 2^{7n-y-x-p-2j-i-9}, & p<x<i=q<j=r \\ 2^{7n-y-x-p-2j-i-10}, & x<p<i=q<j=r \end{cases}$$

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

$$\begin{cases} 2^{7n-2j-i-z-2y-8}, & i=p=x, j=q, r=y \\ 2^{7n-2j-i-z-2y-9}, & i=p=x, j=r, q=y \\ 2^{7n-2j-i-z-2y-9}, & i=p, j=q=x, r=y \\ 2^{7n-2j-i-z-2x-9}, & i=p, j=r=y, q=x \\ 2^{7n-2j-2i-z-x-10}, & i=q=y, j=r, p=x \\ 2^{7n-3j-i-z-x-10}, & i=q, j=r=y, p=x \end{cases}$$

Proof. i) First we prove that $\{i, j\} \subset \{p, q, r\}$ and $j = r < y$.

Suppose that the 0-cube c_1 includes a nonzero element e_1, the 2-cube c_2 includes 4 nonzero elements e_2, e_3, e_4, e_5, and the 1-cube c_3 includes 2 nonzero elements e_6, e_7.

Based on the result by Kurosawa *et al.* (2000), 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 $k_{\min} = 2^{W_H(2^n - L(s))}$. As c_2 is a 2-cube, thus $k_{\min} = 4$, which means that in order to decrease the linear complexity of the 2-cube, we have to change 4 elements. So $L_1(s^{(n)}) = L(c_2) = 2^n - (2^i + 2^j)$, is achieved by changing the nonzero element e_1.

Next, we have to add a new 2-cube with linear complexity $L(c_2)$. If the new 2-cube does not include nonzero element e_1, then we have to change 5 elements. So the new 2-cube has to include the nonzero element e_1. We have to add 3 nonzero elements. Now $s^{(n)}$ becomes a 3-cube, thus $L_3(s^{(n)}) = 2^n - (2^i + 2^j + 2^u)$. So $\{i, j\} \in \{p, q, r\}$. Based on Algorithm 3.2.1 in Section 3.2, the cube with longer edge length will be first removed, so $u < j$.

Similarly, $L_5(s^{(n)})$ is achieved by adding a 1-cube with linear complexity $L(c_3)$, i.e., we need to change 4 nonzero elements of $s^{(n)}$ and add one new nonzero element. As $L_5(s^{(n)}) = 2^n - (2^x + 2^y), 0 \le x < y < n$, thus $L(c_3) = 2^n - 2^y$.

$L_3(s^{(n)}) = 2^n - (2^i + 2^j + 2^u) > L(c_3)$ is immediately followed by $y > r = j$.

Now we will compute the number of sequences $e^{(n)}$ with $W_H(e) = 7$, $L_1(e^{(n)}) = 2^n - (2^i + 2^j)$, $L_3(e^{(n)}) = 2^n - (2^p + 2^q + 2^r)$ and $L_5(e^{(n)}) = 2^n - (2^x + 2^y)$. As c_2 is a 2-cube, so $r = j$. Note that $j = r < y$, there are 8 possible cases:

1. $i = p < q < j = r < x$; 2. $i = p < q < x < j = r$; 3. $i = p, j = r, p < x < q$; 4. $i = p, j = r, x < p$;

5. $i = q < j = r < x$; 6. $i = q, j = r, q < x < r$; 7. $i = q, j = r, p < x < q$; 8. $i = q, j = r, x < p$;

We now cope with these cases respectively.

1. In the case of $i = p < q < j = r < x$.

As the number of 2^{i+1}-periodic binary sequences $e^{(i+1)}$ with linear complexity $2^{i+1} - 2^i = 2^i$ and $W_H(e^{(i+1)}) = 2$ is 2^i. For $j > i$, we aim to obtain 2^j-periodic binary sequences $s^{(j)}$ with linear complexity $2^j - 2^i$ and $W_H(s^{(j)}) = 2$ from above 2^{i+1}-periodic binary sequences

$s^{(i+1)}$. In this case, when the sequence period changes from 2^{i+1} to 2^j, the increase of linear complexity is $2^j - 2^i - (2^{i+1} - 2^i) = 2^{j-1} + 2^{j-2} + \cdots + 2^{i+1}$. Based on Algorithm 3.1.1 in Section 3.1, the number of these $e^{(j)}$ 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 $e^{(j+1)}$ with linear complexity $2^{j+1} - (2^j + 2^i)$ and $W_H(e^{(j+1)}) = 4$ is also 2^{2j-i-2}.

First one nonzero element is added so that $L_1(e^{(j+1)}) = 2^{j+1} - (2^i + 2^j)$ and $L_3(e^{(j+1)}) = 2^{j+1} - (2^i + 2^q + 2^j)$. Note that $i < q < j$, the number of $e^{(j+1)}$ becomes $2^{2j-i-2} \times 2 \times 2^{j-q} = 2^{3j-q-i-1}$.

Suppose that p_1, p_2, p_3, p_4 and p_5 are nonzero elements of $e^{(j+1)}$. Second construct $e^{(x)}$ so that the distance among p_1, p_2, p_3, p_4 and p_5 are unchanged. The number of $e^{(x)}$ becomes $2^{3j-q-i-1} \times (2^5)^{x-j-1} = 2^{5x-2j-q-i-6}$.

Third construct $e^{(x+1)}$ by adding a nonzero element p_6 so that the distance of p_6 and one nonzero element of $e^{(x)}$, say p_1, is 2^x. The number of $e^{(x+1)}$ becomes $2^{5x-2j-q-i-6} \times 5 \times 2^4 = 5 \times 2^{5x-2j-q-i-2}$.

Step 4 we construct $e^{(y)}$ so that the distance among p_1, p_2, p_3, p_4, p_5 and p_6 are unchanged. The number of $e^{(y)}$ becomes $5 \times 2^{5x-2j-q-i-2} \times (2^6)^{y-x-1} = 5 \times 2^{6y-x-2j-q-i-8}$.

Step 5 we construct $e^{(y+1)}$ by adding a nonzero element p_7 so that the distance of p_7 and p_1 or p_6, say p_6, is 2^y. Then $p_1, p_2 p_3$, p_4 and p_5 have 2^5 options. The number of $e^{(y+1)}$ becomes $5 \times 2^{6y-x-2j-q-i-8} \times 2 \times 2^5 = 5 \times 2^{6y-x-2j-q-i-2}$.

Finally the number of sequences $e^{(n)}$ with $W_H(e^{(n)}) = 7$, $L_1(e^{(n)}) = 2^n - (2^i + 2^j)$, $L_3(e^{(n)}) = 2^n - (2^p + 2^q + 2^r)$ and $L_5(e^{(n)}) = 2^n - (2^x + 2^y)$ can be given by

$$5 \times 2^{6y-x-2j-q-i-2} \times (2^7)^{n-y-1} = 5 \times 2^{7n-y-x-2j-q-i-9}.$$

(For example, with a sequence {00000001 00000000 00000001 00110111}, $n = 5, i = 0, j = 2$, $p = 0, q = 1, r = 2$, $x = 3, y = 4$. With 1 bit change, it becomes a 2-cube and a 1-cube: {00000001 00000000 00000001 00110011}. With 3 bits change, it becomes a 3-cube and a 1-cube {00000001 00000000 00000001 11111111}. With 5 bits change, it becomes a 2-cube: {00000001 00000001 00000001 00000001}.)

2. In the case of $i = p < q < x < j = r < y$.

Suppose that $e^{(q)}$ is a 2^q-periodic binary sequence with linear complexity 2^q and $W_H(e^{(q)}) = 1$. Then the number of these $e^{(q)}$ is 2^q. So the number of 2^{q+1}-periodic binary sequences $e^{(q+1)}$ with linear complexity $2^{q+1} - 2^q = 2^q$ and $W_H(e^{(q+1)}) = 2$ is also 2^q.

Step 1 one nonzero element is added to $e^{(q+1)}$ such that $L_1(e^{(q+1)}) = 2^{q+1} - (2^i + 2^q)$. This implies that we place a nonzero element p_3 in $e^{(q+1)}$, so that both the distance of p_1 and p_3, and the distance of p_2 and p_3 are 2^i, where p_1 and p_2 are in $e^{(q+1)}$, and the distance of p_1 and p_2 is 2^q. The number of new $e^{(q+1)}$ becomes $2^q \times \frac{2^{q+1}}{2^{i+1}} = 2^q \times 2^{q-i} = 2^{2q-i}$.

Step 2 we construct $e^{(x)}$ so that $L_1(e^{(x)}) = 2^x - (2^i + 2^q)$. The number of such $e^{(x)}$ becomes $2^{2q-i} \times (2^3)^{x-q-1} = 2^{3x-q-i-3}$.

Step 3 we construct $e^{(x+1)}$ by adding another nonzero element p_4 so that the distance of p_4 and one nonzero element of p_1, p_2 or p_3 is 2^x. There are 3 options. For the convenience of presentation, suppose that the distance of p_4 and p_1 is 2^x. Then p_2 and p_3 have 2^2 options. The number of such $e^{(x+1)}$ becomes $2^{3x-q-i-3} \times 3 \times 2^2$.

Step 4 we construct $e^{(j)}$ so that the distance (based on Definition 2.1) among p_1, p_2, p_3 and p_4 are unchanged. The number of such $e^{(j)}$ becomes $3 \times 2^{3x-q-i-1} \times (2^4)^{j-x-1} = 3 \times 2^{4j-x-q-i-5}$.

Step 5 we construct $e^{(j+1)}$ by adding two nonzero elements p_5, p_6 so that p_1 (or p_2), p_3, p_5 and p_6 constitute a 2-cube with linear complexity $2^{j+1} - (2^i + 2^j)$. The number of $e^{(j+1)}$ becomes $3 \times 2^{4j-x-q-i-5} \times 2 \times 2^2$.

Step 6 we construct $e^{(y)}$ so that the distance (based on Definition 2.1) among p_1, p_2, p_3, p_4, p_5 and p_6 are unchanged. The number of such $e^{(y)}$ becomes $3 \times 2^{4j-x-q-i-2} \times (2^6)^{y-j-1} = 3 \times 2^{6y-2j-x-q-i-8}$.

Step 7 we construct $e^{(y+1)}$ by adding one nonzero element p_7 so that the distance of p_1 (or p_4) and p_7 is 2^y. The number of $e^{(y+1)}$ becomes $3 \times 2^{6y-2j-x-q-i-8} \times 2 \times 2^5$.

Finally the number of sequences $e^{(n)}$ with $W_H(e^{(n)}) = 7$, $L_1(e^{(n)}) = 2^n - (2^i + 2^j)$, $L_3(e^{(n)}) = 2^n - (2^p + 2^q + 2^r)$ and $L_5(e^{(n)}) = 2^n - (2^x + 2^y)$ can be given by

$$3 \times 2^{6y-x-2j-q-i-2} \times (2^7)^{n-y-1} = 3 \times 2^{7n-y-x-2j-q-i-9}.$$

(For sequence {00000000 00010000 00000011 00010111}, $n = 5, i = 0, j = 3$, $p = 0, q = 1, r = 3$, $x = 2, y = 4$. With 1 bit change, it becomes a 2-cube and a 1-cube:

{00000000 00010000 00000011 00010011}. With 3 bits change, it becomes a 3-cube and a 1-cube: {00000000 00010000 00001111 00011111}. With 5 bits change, it becomes a 2-cube: {00000000 00010001 00000000 00010001}.)

Similarly we can obtain results for other cases. In summary, the numbers of sequences $e^{(n)}$ can be given by

$$\begin{cases} 5 \times 2^{7n-y-x-q-2j-i-9}, & i = p < q < j = r < x \\ 3 \times 2^{7n-y-x-q-2j-i-9}, & i = p < q < x < j = r \\ 2^{7n-y-x-q-2j-i-8}, & i = p < x < q < j = r \\ 2^{7n-y-x-q-2j-i-9}, & x < i = p < j = r \\ 5 \times 2^{7n-y-x-p-2j-i-10}, & i = q < j = r < x \\ 3 \times 2^{7n-y-x-p-2j-i-10}, & i = q < x < j = r \\ 2^{7n-y-x-p-2j-i-9}, & p < x < i = q < j = r \\ 2^{7n-y-x-p-2j-i-10}, & x < p < i = q < j = r \end{cases}$$

ii) Suppose that $s^{(n)}$ can be decomposed into one 0-cube c_1, one 2-cube c_2 and one 1-cube c_3, where $L(c_2) > L(c_3)$, $L_1(s^{(n)}) = 2^n - (2^i + 2^j), 0 \le i < j < n$, $L_3(s^{(n)}) = 2^n - (2^p + 2^q + 2^r), 0 \le p < q < r < n$, $L_5(s^{(n)}) = 2^n - (2^x + 2^y + 2^z), 0 \le x < y < z < n$.

Similar to the analysis of i), we know that $\{i, j\} \subset \{p, q, r\}$.

As $L_5(s^{(n)}) = 2^n - (2^x + 2^y + 2^z)$, thus $L_5(s^{(n)})$ is achieved by a 3-cube c'. If c' includes 7 nonzero elements of $s^{(n)}$, then $L_5(s^{(n)}) = L_1(s^{(n)})$, which is a contradiction. If c' includes 6 nonzero elements of $s^{(n)}$, then $L_5(s^{(n)}) = L_3(s^{(n)})$, which is also a contradiction. So c' should only include 5 nonzero elements of $s^{(n)}$. Therefore, $\{p, q\} \subset \{x, y, z\}$ or $\{p, r\} \subset \{x, y, z\}$ or $\{q, r\} \subset \{x, y, z\}$.

Note that $r < z$ (refer to Appendix 1) for the proof). Thus there are 3 possible cases:

1. $p = x, q = y$. 2. $p = x, r = y$. 3. $q = x, r = y$.

Note that $i = x$ and $j = y$ can not be true at the same time (refer to Appendix 2) for the proof). Thus there are 6 possible cases:

1.$i = p = x, j = q, r = y$, 2.$i = p = x, j = r, q = y$, 3.$i = q = y, j = r, p = x$,

4.$i = q, j = r = y, p = x$, 5.$i = p, j = q = x, r = y$, 6.$i = p, j = r = y, q = x$.

We now deal with these cases respectively.

1. In the case of $i = p = x, j = q, r = y$.

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 $W_H(s^{(j)}) = 2$ is obtained from $s^{(i)}$, then the increase of linear complexity is $2^j - 2^i - (2^{i+1} - 2^i) = 2^{j-1} + 2^{j-2} + \cdots + 2^{i+1}$. Based on Algorithm 3.1.1 in Section 3.1, 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}.

It is easy to show that the number of 2^{y+1}-periodic binary sequences $s^{(y+1)}$ with linear complexity $2^{y+1} - (2^j + 2^i)$ and $W_H(s^{(y+1)}) = 4$ is $2^{2j-i-2} \times (2^4)^{y+1-j-1} = 2^{4y-2j-i-2}$.

Next we discuss how many options to add two nonzero elements to $s^{(y+1)}$ such that $L_2(s^{(y+1)}) = 2^{y+1} - (2^i + 2^y)$.

As there exist 2^2 pairs of nonzero elements with distance 2^i in a 2-cube with linear complexity $2^{y+1} - (2^i + 2^j)$, we can construct 2^2 2-cubes with smaller linear complexity $2^{y+1} - (2^i + 2^y)$.

(For example, we can construct {0011 0011}, {1100 1100}, {1001 1001} and {0110 0110} from {0000 1111} with $i = 0, j = 1, y = 2$.)

Therefore, we can construct the sequences $s^{(y+1)}$ (not 2-cube anymore) with $L_2(s^{(y+1)}) = 2^{y+1} - (2^i + 2^y)$, $W_h(s^{(y+1)}) = 6$ and containing a 2-cube with linear complexity $2^{y+1} - (2^i + 2^j)$. As we can obtain the same $s^{(y+1)}$ from 2^2 distinct 2-cubes with linear complexity $2^{y+1} - (2^i + 2^j)$, the total number of such sequences $s^{(y+1)}$ is $2^{4y-2j-i-2} \times 2^2 \times \frac{1}{2^2} = 2^{4y-2j-i-2}$ after calculating the overlaps.

(For example, the sequence {0011 1111} is produced by all of the following sequences {0000 1111}, {0010 1101}, {0001 1110} and {0011 1100}).

Next we construct $s^{(z)}$ so that the distance (based on Definition 2.1) among nonzero ele-

ments of $s^{(y+1)}$ are unchanged. The number of such $s^{(z)}$ becomes $2^{4y-2j-i-2} \times (2^6)^{z-y-1} = 2^{6z-2y-2j-i-8}$.

Suppose that p_1, p_2, p_3, p_4, p_5 and p_6 are nonzero elements of $s^{(z)}$, and p_1, p_2, p_5 and p_6 constitute a 2-cube with linear complexity $2^z - (2^i + 2^y)$. Now we construct $s^{(z+1)}$ by adding nonzero element p_7 so that the distance of p_7 and p_1, p_2, p_5 or p_6 is 2^z. There are 4 options. Then other 5 nonzero elements have 2^5 options. The number of such $s^{(z+1)}$ becomes $2^{6z-2y-2j-i-8} \times 4 \times 2^5 = 2^{6z-2y-2j-i-1}$.

Finally the number of sequences $s^{(n)}$ with $W_H(s^{(n)}) = 7$, $L_1(s^{(n)}) = 2^n - (2^i + 2^j)$, $L_3(s^{(n)}) = 2^n - (2^p + 2^q + 2^r)$ and $L_5(s^{(n)}) = 2^n - (2^x + 2^y + 2^z)$ can be given by

$$2^{6z-2y-2j-i-1} \times (2^7)^{n-z-1} = 2^{7n-z-2y-2j-i-8}.$$

(For example, with a sequence $\{0000\ 0001\ 0011\ 1111\}$, $n = 4, i = 0, j = 1$, $p = 0, q = 1, r = 2$, $x = 0, y = 2, z = 3$. With 1 bit change, it becomes a 2-cube and a 1-cube: $\{0000\ 0001\ 0001\ 1111\}$. With 3 bits change, it becomes a 3-cube: $\{0000\ 0000\ 1111\ 1111\}$. With 5 bits change, it becomes a 3-cube: $\{0011\ 0011\ 0011\ 0011\}$.)

2. In the case of $i = p = x, j = r, q = y$.

The number of sequences $s^{(y+1)}$ with linear complexity $2^{y+1} - (2^i + 2^y)$ and $W_H(s^{(y+1)}) = 4$ is 2^{2y-i-2}.

The number of sequences $s^{(j+1)}$ with linear complexity $2^{j+1} - (2^i + 2^y)$ is $2^{2y-i-2} \times (2^4)^{j-y} = 2^{4j-2y-i-2}$.

Similar to the analysis of case 1, the number of $s^{(j+1)}$ becomes $2^{4j-2y-i-2}$, where $L_2(s^{(j+1)}) = 2^{j+1} - (2^i + 2^j)$, $W_H(s^{(j+1)}) = 6$ and $s^{(j+1)}$ contains a 2-cube c' with $L(c') = 2^{j+1} - (2^i + 2^y)$.

The number of sequences $s^{(z)}$ with $L_2(s^{(z)}) = 2^z - (2^i + 2^j)$ becomes $2^{4j-2y-i-2} \times (2^6)^{z-j-1} = 2^{6z-2j-2y-i-8}$.

While keeping $L_1(s^{(z+1)}) = 2^{z+1} - (2^i + 2^j)$, we have two options to construct $s^{(z+1)}$ from a sequence $s^{(z)}$, such that $L_5(s^{(z+1)}) = 2^{z+1} - (2^i + 2^y + 2^z)$. The number of such sequences $s^{(z+1)}$ becomes $2^{6z-2j-2y-i-8} \times 2 \times 2^5 = 2^{6z-2j-2y-i-2}$.

Finally the number of sequences $s^{(n)}$ with $W_H(s^{(n)}) = 7$, $L_1(s^{(n)}) = 2^n - (2^i + 2^j)$,

$L_3(s^{(n)}) = 2^n - (2^p + 2^q + 2^r)$ and $L_5(s^{(n)}) = 2^n - (2^x + 2^y + 2^z)$ can be given by

$$2^{6z-2j-2y-i-2} \times (2^7)^{n-z-1} = 2^{7n-z-2y-2j-i-9}.$$

(For sequence $\{0000\ 0001\ 0110\ 1111\}$, $n = 4, i = 0, j = 2$, $p = 0, q = 1, r = 2$, $x = 0, y = 1, z = 3$. With 1 bit change, it becomes a 2-cube and a 1-cube: $\{0000\ 0001\ 0110\ 0111\}$. With 3 bits change, it becomes a 3-cube $\{0000\ 0000\ 1111\ 1111\}$. With 5 bits change, it becomes a 3-cube: $\{0000\ 1111\ 0000\ 1111\}$.)

We can obtain results for other cases similarly. Finally, the numbers of sequences $e^{(n)}$ can be given by

$$\begin{cases} 2^{7n-2j-i-z-2y-8}, & i = p = x, j = q, r = y \\ 2^{7n-2j-i-z-2y-9}, & i = p = x, j = r, q = y \\ 2^{7n-2j-i-z-2y-9}, & i = p, j = q = x, r = y \\ 2^{7n-2j-i-z-2x-9}, & i = p, j = r = y, q = x \\ 2^{7n-2j-2i-z-x-10}, & i = q = y, j = r, p = x \\ 2^{7n-3j-i-z-x-10}, & i = q, j = r = y, p = x \end{cases}$$

This completes the proof. □

Finally, we consider the case that $s^{(n)}$ can be decomposed into one 0-cube c_1 one 1-cube c_2 and one 2-cube c_3, where $L(c_2) > L(c_3)$.

Theorem 5.1.3 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 1-cube c_2 and one 2-cube c_3, where $L(c_2) > L(c_3)$. We have the following situations.

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

$$\begin{cases} 2^{7n-2j-i-2z-y-8}, & i = p = x, j = q < y, r = z \\ 2^{7n-2j-i-2z-x-10}, & i = p < x, j = q = y, r = z \\ 2^{7n-2j-i-2z-y-9}, & i = p, j = q = x, r = z \\ 2^{7n-3j-i-x-y-10}, & i = p < x, j = r = z, q = y \\ 2^{7n-3j-i-x-y-9}, & i = p, j = r = z, q = x \\ 2^{7n-3j-i-x-y-10}, & i = q < y, j = r = z, p = x \end{cases}$$

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

$$\begin{cases} 3 \times 2^{7n-2q-y-p-j-i-9}, & p = x < i < j < y < q = z \\ 3 \times 2^{7n-2q-y-p-j-i-9}, & i < p = x < j < y < q = z \\ 3 \times 2^{7n-2q-y-p-j-i-9}, & i < j < p = x < y < q = z \\ 2^{7n-2q-y-p-j-i-8}, & p = x < i < y < j < q = z \\ 2^{7n-2q-y-p-j-i-8}, & i < p = x < y < j < q = z \\ 2^{7n-2q-y-p-j-i-9}, & p = x < y < i < j < q = z \\ 2^{7n-2q-x-p-j-i-10}, & x < p = y < i < j < q = z \\ 2^{7n-2q-x-p-j-i-10}, & x < i < p = y < j < q = z \\ 2^{7n-2q-x-p-j-i-9}, & i < x < p = y < j < q = z \\ 2^{7n-2q-y-x-j-i-9}, & i < x < j < p = y < q = z \\ 3 \times 2^{7n-2q-y-x-j-i-10}, & i < j < x < p = y < q = z \\ 2^{7n-2j-i-2z-p-9}, & i = x > p, j = y, q = z \\ 2^{7n-2j-i-2z-p-9}, & i = x < p, j = y, q = z \\ 2^{7n-2j-i-2z-p-9}, & p = x, j = y, q = z \\ 2^{7n-2j-i-2z-y-10}, & j = x, p = y, q = z \end{cases}$$

Proof. Suppose that $s^{(n)}$ can be decomposed by Algorithm 3.2.1 in Section 3.2 into one 0-cube c_1 (one nonzero element e_1), one 1-cube c_2 (two nonzero elements e_2, e_3) and one 2-cube c_3 (four nonzero elements e_4, e_5, e_6, e_7) with linear complexity $2^n - (2^u + 2^v), u < v$, and $L(c_2) > L(c_3)$. Let 2^d be the maximum of $\{D(e_i, e_j) | 1 \le i \le 3, 4 \le j \le 7\}$, where $D(e_i, e_j)$ denotes the distance of e_i and e_j based on Definition 2.1. Without loss of generality, suppose that $D(e_1, e_4) = 2^d$. Then one can change e_2, e_3, and add e_8, e_9, e_{10}, such that e_1, e_8, e_9 and e_{10} constitute a 2-cube c_4 with linear complexity $2^n - (2^u + 2^v)$, and c_3 and c_4 constitute a 3-cube. So $L_5(s^{(n)}) = 2^n - (2^x + 2^y + 2^z)$, where $d \in \{x, y\}$. The 3-cube with linear complexity $2^n - (2^x + 2^y + 2^z)$ must include four nonzero elements e_4, e_5, e_6, e_7 and one nonzero element of e_1, e_2, e_3.

i) Suppose that $L_1(s^{(n)}) = 2^n - (2^i + 2^j), 0 \le i < j < n$, $L_3(s^{(n)}) = 2^n - (2^p + 2^q + 2^r), 0 \le p < q < r < n$, $L_5(s^{(n)}) = 2^n - (2^x + 2^y + 2^z), 0 \le x < y < z < n$.

If the distance of one pair of nonzero elements of e_1, e_2, e_3 is u or v. Assume $D(e_1, e_2) = 2^u$. Then one can change e_3, and add e_8, e_9, so that e_1, e_2, e_8 and e_9 constitute a 2-cube c_4 with linear complexity $2^n - (2^u + 2^v)$, and c_3 and c_4 constitute a 3-cube. Thus $L_3(s^{(n)}) = 2^n - (2^p + 2^q + 2^r)$, where $u, v \in \{p, q, r\}$. As $L_3(s^{(n)})$ is achieved by a 3-cube containing c_3, thus $r = z = v$. In this case, there are 6 possible cases as follows.

1. $i = p = x, j = q < y, r = z$, 2. $i = p < x, j = q = y, r = z$, 3. $i = p, j = q = x, r = z$,

4. $i = p < x, j = r = z, q = y$, 5. $i = p, j = r = z, q = x$, 6. $i = q < y, j = r = z, p = x$.

We now deal with these cases respectively.

1. In the case of $i = p = x, j = q < y, r = z$.

It is easy to show that the number of 2^{z+1}-periodic binary sequences $s^{(z+1)}$ with linear complexity $2^{z+1} - (2^j + 2^i)$ and $W_H(s^{(z+1)}) = 4$ is $2^{2j-i-2} \times (2^4)^{z+1-j-1} = 2^{4z-2j-i-2}$.

Suppose that the nonzero elements of $s^{(z+1)}$ are p_1, p_2, p_3 and p_4. Next we add two nonzero elements to $s^{(z+1)}$ so that $L_2(s^{(z+1)}) = 2^{z+1} - (2^i + 2^z)$. As there exist 2^2 pairs of nonzero elements with distance 2^i in a 2-cube with linear complexity $2^{z+1} - (2^i + 2^j)$, we can construct 2^2 2-cubes with linear complexity $2^{z+1} - (2^i + 2^z)$. (For example, we can construct {0011 0011}, {1100 1100}, {1001 1001} and {0110 0110} from {0000 1111} with $i = 0, j = 1, z = 2$.)

Therefore, we can construct the sequences $s^{(z+1)}$ (not 2-cube anymore) with $L_2(s^{(z+1)}) = 2^{z+1} - (2^i + 2^z)$, $W_h(s^{(z+1)}) = 6$ and containing a 2-cube with linear complexity $2^{z+1} - (2^i + 2^j)$. As we can obtain the same $s^{(z+1)}$ from 2^2 distinct 2-cubes with linear complexity $2^{z+1} - (2^i + 2^j)$, the total number of such sequences $s^{(z+1)}$ is $2^{4z-2j-i-2} \times 2^2 \times \frac{1}{2^2} = 2^{4z-2j-i-2}$ after calculating the overlaps.

(For example, the sequence {0011 1111} is produced by all of the following sequences {0000 1111}, {0010 1101}, {0001 1110} and {0011 1100}).

Further we add one nonzero element to $s^{(z+1)}$ such that $L_5(s^{(z+1)}) = 2^{z+1} - (2^i + 2^y + 2^z)$. Suppose that $s^{(z+1)}$ now has two more nonzero elements p_5 and p_6. Add one nonzero element p_7 such that the distance $D(p_5, p_7) = 2^y$ or $D(p_6, p_7) = 2^y$. Thus the number of $s^{(z+1)}$ becomes $2^{4z-2j-i-2} \times 2 \times 2^{z-y} = 2^{5z-y-2j-i-1}$.

Finally the number of sequences $s^{(n)}$ with $W_H(s^{(n)}) = 7$, $L_1(s^{(n)}) = 2^n - (2^i + 2^j)$, $L_3(s^{(n)}) = 2^n - (2^p + 2^q + 2^r)$ and $L_5(s^{(n)}) = 2^n - (2^x + 2^y + 2^z)$ can be given by

$$2^{5z-y-2j-i-1} \times (2^7)^{n-z-1} = 2^{7n-2j-i-2z-y-8}.$$

(For sequence {0000 0011 0001 1111}, $n = 4, i = 0, j = 1$, $p = 0, q = 1, r = 3$, $x = 0, y = 2, z = 3$. With 1 bit change, it becomes two 2-cubes: {0000 0011 0011 1111}. With 3 bits

change, it becomes a 3-cube {0000 1111 0000 1111}. With 5 bits change, it becomes a 3-cube: {0011 0011 0011 0011}.)

2. In the case of $i = p < x, j = q = y, r = z$.

It is easy to show that the number of 2^{z+1}-periodic binary sequences $s^{(z+1)}$ with linear complexity $2^{z+1} - (2^j + 2^i)$ and $W_H(s^{(z+1)}) = 4$ is $2^{2j-i-2} \times (2^4)^{z+1-j-1} = 2^{4z-2j-i-2}$.

Suppose that the nonzero elements of $s^{(z+1)}$ are p_1, p_2, p_3 and p_4. Next we add two nonzero elements to $s^{(z+1)}$ so that $L_2(s^{(z+1)}) = 2^{z+1} - (2^j + 2^z)$. From a 2-cube with linear complexity $2^{z+1} - (2^i + 2^j)$, we have two 2-cubes with linear complexity $2^{z+1} - (2^j + 2^z)$.

Next we add two nonzero elements to $s^{(z+1)}$ so that $L_2(s^{(z+1)}) = 2^{z+1} - (2^j + 2^z)$, $W_h(s^{(z+1)}) = 6$ and $s^{(z+1)}$ contains a 2-cube c' with $L(c') = 2^{z+1} - (2^i + 2^j)$.

As we can obtain the same $s^{(z+1)}$ from 2^2 distinct 2-cubes with linear complexity $2^{z+1} - (2^i + 2^j)$, the total number of such sequences $s^{(z+1)}$ is $2^{4z-2j-i-2} \times 2 \times \frac{1}{2^2} = 2^{4z-2j-i-3}$ after calculating the overlaps.

(For example, the sequence {0011 1111} is produced by all of the following sequences {0000 1111}, {0010 1101}, {0001 1110} and {0011 1100}).

Further add one nonzero element to $s^{(z+1)}$ so that $L_5(s^{(z+1)}) = 2^{z+1} - (2^x + 2^j + 2^z)$. Suppose that $s^{(z+1)}$ now has two more nonzero elements p_5 and p_6. Add one nonzero element p_7 such that the distance $D(p_5, p_7) = 2^x$ (at the same time $D(p_6, p_7) = 2^x$). Thus the number of $s^{(z+1)}$ becomes $2^{4z-2j-i-3} \times 2^{z-x} = 2^{5z-x-2j-i-3}$.

Finally the number of these $s^{(n)}$ can be given by

$$2^{5z-x-2j-i-3} \times (2^7)^{n-z-1} = 2^{7n-2j-i-2z-x-10}.$$

(For sequence {0001 0001 0011 0111}, $n = 4, i = 0, j = 2$, $p = 0, q = 2, r = 3$, $x = 1, y = 2, z = 3$. With 1 bit change, it becomes two 2-cubes: {0001 0001 0111 0111}. With 3 bits change, it becomes a 3-cube {0011 0011 0011 0011}. With 5 bits change, it becomes a 3-cube: {0101 0101 0101 0101}.)

3. In the case of $i = p, j = q = x, r = z$. Note that from a 2-cube with linear complexity $2^{y+1} - (2^i + 2^j)$, we can have two 2-cubes with linear complexity $2^{y+1} - (2^j + 2^y)$. Thus

the number of these e can be given by

$$2^{4y-2j-i-2} \times 2 \times \frac{1}{2^2} \times 2 \times (2^5)^{z-y-1} \times 2^2 \times 2^3 \times (2^7)^{n-z-1} = 2^{7n-2j-i-2z-y-9}.$$

(For sequence $\{0000\ 0101\ 0001\ 1111\}$, $n = 4, i = 0, j = 1$, $p = 0, q = 1, r = 3$, $x = 1, y = 2, z = 3$. With 1 bit change, it becomes two 2-cubes: $\{0000\ 0101\ 0101\ 1111\}$. With 3 bits change, it becomes a 3-cube $\{0000\ 1111\ 0000\ 1111\}$. With 5 bits change, it becomes a 3-cube: $\{0101\ 0101\ 0101\ 0101\}$.)

4. In the case of $i = p < x, q = y, j = r = z$. The number of these sequences e can be given by

$$2^{2j-i-2} \times 2 \times 2^{j-x-1} \times 2^{j-y-1} \times \frac{1}{2} \times 2 \times (2^7)^{n-j-1} = 2^{7n-3j-i-x-y-10}.$$

(For sequence $\{0001\ 0111\ 0001\ 0011\}$, $n = 4, i = 0, j = 3$, $p = 0, q = 2, r = 3$, $x = 1, y = 2, z = 3$. With 1 bit change, it becomes two 2-cubes: $\{0001\ 0111\ 0001\ 0111\}$. With 3 bits change, it becomes a 3-cube $\{0011\ 0011\ 0011\ 0011\}$. With 5 bits change, it becomes a 3-cube: $\{0101\ 0101\ 0101\ 0101\}$.)

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

$$2^{2j-i-2} \times 2 \times 2^{j-x-1} \times 2^{j-y-1} \times \frac{1}{2} \times 2^2 \times (2^7)^{n-j-1} = 2^{7n-3j-i-x-y-9}.$$

(For sequence $\{0000\ 0111\ 0001\ 0111\}$, $n = 4, i = 0, j = 3$, $p = 0, q = 1, r = 3$, $x = 1, y = 2, z = 3$. With 1 bit change, it becomes two 2-cubes: $\{0001\ 0111\ 0001\ 0111\}$. With 3 bits change, it becomes a 3-cube: $\{0000\ 1111\ 0000\ 1111\}$. With 5 bits change, it becomes a 3-cube: $\{0101\ 0101\ 0101\ 0101\}$.)

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

$$2^{2j-i-2} \times 2^{j-x-1} \times 2^{j-y-1} \times \frac{1}{2} \times 2^2 \times (2^7)^{n-j-1} = 2^{7n-3j-i-x-y-10}.$$

(For sequence $\{0001\ 1010\ 0001\ 1011\}$, $n = 4, i = 1, j = 3$, $p = 0, q = 1, r = 3$, $x = 0, y = 2, z = 3$. With 1 bit change, it becomes two 2-cubes: $\{0001\ 1011\ 0001\ 1011\}$. With 3 bits change, it becomes a 3-cube: $\{0001\ 1110\ 0001\ 1110\}$. With 5 bits change, it becomes a 3-cube: $\{0011\ 0011\ 0011\ 0011\}$.)

ii) Suppose that $L_1(s^{(n)}) = 2^n - (2^i + 2^j), 0 \leq i < j < n$, $L_3(s^{(n)}) = 2^n - (2^p + 2^q), 0 \leq p < q < n$, $L_5(s^{(n)}) = 2^n - (2^x + 2^y + 2^z), 0 \leq x < y < z < n$. Then the distance among

nonzero elements of e_1, e_2, e_3 (see notations in the beginning of the proof) is neither u nor v. As $L_3(s^{(n)})$ is achieved by c_3, so $L_3(s^{(n)}) = 2^n - (2^p + 2^q) = 2^n - (2^u + 2^v)$, thus $q = z = v$.

If $s^{(n)}$ contains only one 2-cube c_3, then both i and j are not in $\{p, q\}$, $\{p, q\} \subset \{x, y, z\}$. There are 11 possible cases as follows.

1. $p = x < i < j < y$, 2. $i < p = x < j < y$, 3. $i < j < p = x < y$, 4. $p = x < i < y < j$,

5. $i < p = x < y < j$, 6. $p = x < y < i < j$, 7. $x < p = y < i < j$, 8. $x < i < p = y < j$,

9. $i < x < p = y < j$, 10. $i < x < j < p = y$, 11. $i < j < x < p = y$.

If $s^{(n)}$ contains two distinct 2-cubes. There are another 4 possible cases as follows (refer to Appendix 9) for the proof).

12. $i = x > p, j = y, q = z$, 13. $i = x < p, j = y, q = z$,

14. $p = x, j = y, q = z$, 15. $j = x, p = y, q = z$.

1. Now consider the case of $p = x < i < j < y < q = z$ as follows.

Suppose that $e^{(j)}$ is a 2^j-periodic binary sequence with linear complexity 2^j and $W_H(e^{(j)}) = 1$. Then the number of these $e^{(j)}$ is 2^j. So the number of 2^{j+1}-periodic binary sequences $e^{(j+1)}$ with linear complexity $2^{j+1} - 2^j = 2^j$ and $W_H(e^{(j+1)}) = 2$ is also 2^j.

First one nonzero element is added to $e^{(j+1)}$ such that $L_1(e^{(j+1)}) = 2^{j+1} - (2^i + 2^j)$. This implies that we place a nonzero element p_3 in $e^{(j+1)}$, so that both the distance of p_1 and p_3, and the distance of p_2 and p_3 are 2^i, where p_1 and p_2 are in $e^{(j+1)}$, and the distance of p_1 and p_2 is 2^j. The number of new $e^{(j+1)}$ becomes $2^j \times \frac{2^{j+1}}{2^{i+1}} = 2^j \times 2^{j-i} = 2^{2j-i}$.

Second construct $e^{(y)}$ so that $L_1(e^{(y)}) = 2^y - (2^i + 2^j)$. The number of such $e^{(y)}$ becomes $2^{2j-i} \times (2^3)^{y-j-1} = 2^{3y-j-i-3}$.

Third construct $e^{(y+1)}$ by adding another nonzero element p_4 so that the distance of p_4 and one nonzero element of p_1, p_2 or p_3 is 2^y. There are 3 options. For the convenience of presentation, suppose that the distance of p_4 and p_1 is 2^y. Then p_2 and p_3 have 2^2 options. The number of such $e^{(y+1)}$ becomes $2^{3y-j-i-3} \times 3 \times 2^2$. Further add a nonzero element p_5 so that the distance of p_4 and p_5 is 2^p. Thus the number of $e^{(y+1)}$ becomes

$3 \times 2^{3y-j-i-1} \times 2^{y-p}$.

Step 4 we construct $e^{(q)}$ so that the distance (based on Definition 2.1) among p_1, p_2, p_3, p_4 and p_5 are unchanged. The number of such $e^{(q)}$ becomes $3 \times 2^{4y-p-j-i-1} \times (2^5)^{q-y-1} = 3 \times 2^{5q-y-p-j-i-6}$.

Step 5 we construct $e^{(q+1)}$ by adding two nonzero elements p_6, p_7, so that p_4 (or p_1), p_5, p_6 and p_7 constitute a 2-cube with linear complexity $2^{q+1} - (2^p + 2^q)$. The number of $e^{(q+1)}$ becomes $3 \times 2^{5q-y-p-j-i-6} \times 2 \times 2^3$.

Finally the number of sequences $e^{(n)}$ with $W_H(e^{(n)}) = 7$, $L_1(e^{(n)}) = 2^n - (2^i + 2^j)$, $L_3(e^{(n)}) = 2^n - (2^p + 2^q)$ and $L_5(e^{(n)}) = 2^n - (2^x + 2^y + 2^z)$ can be given by

$$3 \times 2^{5q-y-p-j-i-2} \times (2^7)^{n-q-1} = 3 \times 2^{7n-q-y-p-j-i-9}$$

(For sequence {11000000 10101000 11000000 00000000}, $n = 5, i = 1, j = 2$, $p = x = 0, y = 3$, $q = z = 4$. With 1 bit change, it becomes one 2-cube and one 2-cube: {11000000 10101010 11000000 00000000}. With 3 bits change, it becomes one 2-cube: {11000000 00000000 11000000 00000000} With 5 bits change, it becomes a 3-cube: {11000000 11000000 11000000 11000000})

2. For the case of $i < p = x < j < y < q = z$, here only give the brief construction process.

$e^{(y)} : 2^{2j-i} \times (2^3)^{y-j-1} \Longrightarrow e^{(y+1)} : 2^{3y-j-i-3} \times 3 \times 2^2 \times 2^{y-p}$

$\Longrightarrow e^{(q)} : 3 \times 2^{4y-p-j-i-1} \times (2^5)^{q-y-1} \Longrightarrow e^{(q+1)} : 3 \times 2^{5q-y-p-j-i-6} \times 2 \times 2^3 = 3 \times 2^{5q-y-p-j-i-2}$.

3. For the case of $i < j < p = x < y < q = z$, here only give the brief construction process.

$e^{(y)} : 2^{2j-i} \times (2^3)^{y-j-1} \Longrightarrow e^{(y+1)} : 2^{3y-j-i-3} \times 3 \times 2^2 \times 2^{y-p}$

$\Longrightarrow e^{(q)} : 3 \times 2^{4y-p-j-i-1} \times (2^5)^{q-y-1} \Longrightarrow e^{(q+1)} : 3 \times 2^{5q-y-p-j-i-6} \times 2 \times 2^3 = 3 \times 2^{5q-y-p-j-i-2}$.

4. For the case of $p = x < i < y < j < q = z$, here only give the brief construction process.

$e^{(j+1)} : 2^{2j-i} \times 2 \times 2^{j-y} \times 2^{j-p} = 2^{4j-y-p-i+1}$

$\Longrightarrow e^{(q)}: 2^{4j-y-p-i+1} \times (2^5)^{q-j-1} \Longrightarrow e^{(q+1)}: 2^{5q-y-p-j-i-4} \times 2^3 = 2^{5q-y-p-j-i-1}$.

5. For the case of $i < p = x < y < j < q = z$, here only give the brief construction process.

$e^{(j+1)}: 2^{2j-i} \times 2 \times 2^{j-y} \times 2^{j-p} = 2^{4j-y-p-i+1}$

$\Longrightarrow e^{(q)}: 2^{4j-y-p-i+1} \times (2^5)^{q-j-1} \Longrightarrow e^{(q+1)}: 2^{5q-y-p-j-i-4} \times 2^3 = 2^{5q-y-p-j-i-1}$.

6. For the case of $p = x < y < i < j < q = z$, here only give the brief construction process.

$e^{(j+1)}: 2^{2j-i} \times 2^{j-y} \times 2^{j-p} = 2^{4j-y-p-i}$

$\Longrightarrow e^{(q)}: 2^{4j-y-p-i} \times (2^5)^{q-j-1} \Longrightarrow e^{(q+1)}: 2^{5q-y-p-j-i-5} \times 2^3 = 2^{5q-y-p-j-i-2}$.

7. For the case of $x < p = y < i < j < q = z$, here only give the brief construction process.

$e^{(i+1)}: 2^{2p-x} \times (2^3)^{i-p-1} \times 2^2 = 2^{3i-x-p-1} \Longrightarrow e^{(j+1)}: 2^{3i-x-p-1} \times (2^4)^{j-i-1} \times 2 \times 2^3$

$\Longrightarrow e^{(q)}: 2^{4j-x-p-i-1} \times (2^5)^{q-j-1} \Longrightarrow e^{(q+1)}: 2^{5q-x-p-j-i-6} \times 2^3 = 2^{5q-x-p-j-i-3}$.

8. For the case of $x < i < p = y < j < q = z$, here only give the brief construction process.

$e^{(p+1)}: 2^{2i-x} \times (2^3)^{p-i-1} \times 2^2 = 2^{3p-x-i-1} \Longrightarrow e^{(j+1)}: 2^{3p-x-i-1} \times (2^4)^{j-p-1} \times 2 \times 2^3$

$\Longrightarrow e^{(q)}: 2^{4j-x-p-i-1} \times (2^5)^{q-j-1} \Longrightarrow e^{(q+1)}: 2^{5q-x-p-j-i-6} \times 2^3 = 2^{5q-x-p-j-i-3}$.

9. For the case of $i < x < p = y < j < q = z$, here only give the brief construction process.

$e^{(p+1)}: 2^{2x-i} \times (2^3)^{p-i-1} \times 2 \times 2^2 = 2^{3p-x-i} \Longrightarrow e^{(j+1)}: 2^{3p-x-i} \times (2^4)^{j-p-1} \times 2 \times 2^3$

$\Longrightarrow e^{(q)}: 2^{4j-x-p-i} \times (2^5)^{q-j-1} \Longrightarrow e^{(q+1)}: 2^{5q-x-p-j-i-5} \times 2^3 = 2^{5q-x-p-j-i-2}$.

10. For the case of $i < x < j < p = y << q = z$, here only give the brief construction process.

$e^{(j+1)}: 2^{2x-i} \times (2^3)^{j-i-1} \times 2 \times 2^2 = 2^{3j-x-i} \Longrightarrow e^{(y+1)}: 2^{3j-x-i} \times (2^4)^{y-j-1} \times 2 \times 2^3$

$\Longrightarrow e^{(q)}: 2^{4y-j-x-i} \times (2^5)^{q-j-1} \Longrightarrow e^{(q+1)}: 2^{5q-y-x-j-i-5} \times 2^3 = 2^{5q-y-x-j-i-2}$.

11. For the case of $i < j < x < p = y < q = z$, here only give the brief construction process.

$e^{(x+1)} : 2^{2j-i} \times (2^3)^{x-j-1} \times 3 \times 2^2 = 3 \times 2^{3x-j-i-1} \Longrightarrow e^{(y+1)} : 3 \times 2^{3x-j-i-1} \times (2^4)^{y-x-1} \times 2 \times 2^3$

$\Longrightarrow e^{(q)} : 3 \times 2^{4y-x-j-i-1} \times (2^5)^{q-y-1} \Longrightarrow e^{(q+1)} : 3 \times 2^{5q-y-x-j-i-6} \times 2^3 = 3 \times 2^{5q-y-x-j-i-3}$.

12. For the case of $i = x > p, j = y, q = z$. From a 2-cube with linear complexity $2^{j+1} - (2^i + 2^j)$, we have $2^{j-p} \times 2^2$ 1-cubes with linear complexity $2^{j+1} - 2^p$. Thus the number of these e can be given by

$$2^{2j-i-2} \times 2^{j-p} \times 2^2 \times (2^5)^{z-j-1} \times 2^3 \times (2^7)^{n-z-1} = 2^{7n-2j-i-2z-p-9}.$$

(For sequence {0000 0011 1010 1011}, $n = 4, i = 1, j = 2, p = 0, q = 3, x = 1, y = 2, z = 3$. With 1 bit change, it becomes a 2-cube and a 1-cube: {0000 0001 1010 1011}. With 3 bits change, it becomes a 2-cube {0000 0011 0000 0011}. With 5 bits change, it becomes a 3-cube: {1010 1010 1010 1010}.)

13. For the case of $i = x < p, j = y, q = z$. From a 2-cube with linear complexity $2^{j+1} - (2^i + 2^j)$, we have $2^{j+1-p-1} \times 2$ sequences containing a 1-cube with linear complexity $2^{j+1} - 2^p$. Thus the number of these e can be given by

$$2^{2j-i-2} \times 2^{j-p} \times 2^2 \times (2^5)^{z-j-1} \times 2^3 \times (2^7)^{n-z-1} = 2^{7n-2j-i-2z-p-9}.$$

(For sequence {0000 0011 0110 0111}, $n = 4, i = 0, j = 2, p = 1, q = 3, x = 0, y = 2, z = 3$. With 1 bit change, it becomes a 2-cube and a 1-cube: {0000 0001 0110 0111}. With 3 bits change, it becomes two 2-cubes {0010 0111 0010 0111}. With 5 bits change, it becomes a 3-cube: {0011 0011 0011 0011}.)

14. For the case of $p = x, j = y, q = z$. The number of these e can be given by

$$2^{2j-i-2} \times 2^{j-p} \times 2^2 \times (2^5)^{z-j-1} \times 2^3 \times (2^7)^{n-z-1} = 2^{7n-2j-i-2z-p-9}.$$

(For sequence {0000 0101 0011 0111}, $n = 4, i = 0, j = 2, p = 1, q = 3, x = 1, y = 2, z = 3$. With 1 bit change, it becomes a 2-cube and a 1-cube: {0000 0100 0011 0111}. With 3 bits change, it becomes a 2-cube {0000 0101 0000 0101}. With 5 bits change, it becomes a 3-cube: {0101 0101 0101 0101}.)

15. For the case of $j = x, p = y, q = z$, the number of these e can be given by

$$2^{4z-2j-i-6} \times 4 \times 2^{z-y-1} \times \frac{1}{2} \times 2^3 \times (2^7)^{n-z-1} = 2^{7n-2j-i-2z-y-10}.$$

(For sequence $\{0001\ 0001\ 0001\ 1111\}$, $n = 4, i = 0, j = 1$, $p = 2, q = 3$, $x = 1, y = 2, z = 3$. With 1 bit change, it becomes a 2-cube and a 1-cube: $\{0001\ 0001\ 0000\ 1111\}$. With 3 bits change, it becomes a 2-cube $\{0001\ 0001\ 0001\ 0001\}$. With 5 bits change, it becomes a 3-cube: $\{0101\ 0101\ 0101\ 0101\}$.)

In summary, the number of 2^n-periodic binary sequences $s^{(n)}$ can be given by

$$\begin{cases}
3 \times 2^{7n-2q-y-p-j-i-9}, & p = x < i < j < y < q = z \\
3 \times 2^{7n-2q-y-p-j-i-9}, & i < p = x < j < y < q = z \\
3 \times 2^{7n-2q-y-p-j-i-9}, & i < j < p = x < y < q = z \\
2^{7n-2q-y-p-j-i-8}, & p = x < i < y < j < q = z \\
2^{7n-2q-y-p-j-i-8}, & i < p = x < y < j < q = z \\
2^{7n-2q-y-p-j-i-9}, & p = x < y < i < j < q = z \\
2^{7n-2q-x-p-j-i-10}, & x < p = y < i < j < q = z \\
2^{7n-2q-x-p-j-i-10}, & x < i < p = y < j < q = z \\
2^{7n-2q-x-p-j-i-9}, & i < x < p = y < j < q = z \\
2^{7n-2q-y-x-j-i-9}, & i < x < j < p = y < q = z \\
3 \times 2^{7n-2q-y-x-j-i-10}, & i < j < x < p = y < q = z \\
2^{7n-2j-i-2z-p-9}, & i = x > p, j = y, q = z \\
2^{7n-2j-i-2z-p-9}, & i = x < p, j = y, q = z \\
2^{7n-2j-i-2z-p-9}, & p = x, j = y, q = z \\
2^{7n-2j-i-2z-y-10}, & j = x, p = y, q = z
\end{cases}$$

This completes the proof. □

To verify Theorem 5.1.1, Theorem 5.1.2 and Theorem 5.1.3, we give the complete 2^n-periodic binary sequence distribution with the given k-error linear complexity profile of $0 = L_7(s^{(n)}) < L_5(s^{(n)}) < L_3(s^{(n)}) < L_1(s^{(n)}) < L(s^{(n)}) = 2^n$ for $n = 5$, which is checked by a computer program (refer to Appendix 10) for the detail). In general, with higher linear complexity and k-error linear complexity, the number of the sequences will increases. However, we noticed some interesting exceptions in the example.

5.2 The k-error linear complexity profile having descent points 2, 4, 6 and 8

Based on the Games-Chan algorithm (Games and Chan, 1983) and the cube theory of Chapter 3, we illustrated a constructive approach for determining the distribution of 2^n-periodic binary sequences with the given k-error linear complexity profile of $0 = L_7(s^{(n)}) < L_5(s^{(n)}) < L_3(s^{(n)}) < L_1(s^{(n)}) < L(s^{(n)}) = 2^n$. Suppose that $0 = L_8(s^{(n)}) < L_6(s^{(n)}) < L_4(s^{(n)}) < L_2(s^{(n)}) < L(s^{(n)}) < 2^n$. Using this approach, we now discuss some special cases. In this case, $L(s^{(n)})$ is variable, so it is much more difficult to have a complete characterization.

Theorem 5.2.1 Let $s^{(n)}$ be a 2^n-periodic binary sequence with linear complexity less than 2^n and $0 = L_8(s^{(n)}) < L_6(s^{(n)}) < L_4(s^{(n)}) < L_2(s^{(n)}) < L(s^{(n)}) < 2^n$. Suppose that $s^{(n)}$ can be decomposed into one 2-cube and two 1-cubes, $L(s^{(n)}) = 2^n - 2^{i_0}, 0 \le i_0 < n$, $L_2(s^{(n)}) = 2^n - (2^i + 2^j), 0 \le i < j < n$, $L_4(s^{(n)}) = 2^n - (2^p + 2^q + 2^r), 0 \le p < q < r < n$ and $L_6(e) = 2^n - (2^x + 2^y + 2^z), 0 \le x < y < z < n$. Then the number of 2^n-periodic binary sequences $s^{(n)}$ can be given by

$$\begin{cases} 2^{8n-2z-2j-2q-p-9}, & i_0 = p, i = x, q < j = y, r = z \\ 2^{8n-2z-3q-p-i-9}, & i_0 = p, i = x, q = j = y, r = z \\ 2^{8n-4j-q-p-i-8}, & i_0 = p, i = x, q = y, j = r = z \\ 2^{8n-2z-2j-2q-p-10}, & i_0 = q, i = p = x, j = y, r = z \\ 2^{8n-z-r-2j-2q-p-9}, & i_0 = p, i = x, q < j = y < r < z \\ 2^{8n-z-2j-2q-2p-14}, & i_0 = p, i = x, q < j < y = r < z \end{cases}$$

Proof. As $0 = L_8(s^{(n)}) < L_6(s^{(n)}) < L_4(s^{(n)}) < L_2(s^{(n)}) < L(s^{(n)}) < 2^n$, $s^{(n)}$ can be decomposed into one 2-cube and two 1-cubes or four 1-cubes. Here we only discuss six special cases of one 2-cube and two 1-cubes.

1. In the case of $i_0 = p, i = x, q < j = y, r = z$. It is easy to show that there are two kinds of sequences $s^{(n)}$, illustrated by the following examples, meeting the condition of $L(s^{(n)}) = 2^n - 2^{i_0}$, $L_2(s^{(n)}) = 2^n - (2^i + 2^j)$, $L_4(s^{(n)}) = 2^n - (2^p + 2^q + 2^r)$ and $L_6(e) = 2^n - (2^x + 2^y + 2^z)$.

A) {0000 0011 0101 1111}; B) {0000 0101 0011 1111}, where $n = 4, i_0 = 0, i = 1, j = 2$, $p = 0, q = 1, r = 3$, $x = 1, y = 2, z = 3$.

We now derive the counting formula of 2^n-periodic binary sequences of type A.

As $p < q < j$, the number of 2^j-periodic binary sequences $s^{(j)}$ with linear complexity $2^j - (2^q + 2^p)$ and $W_H(s^{(j)}) = 4$ is $2^{4j-2q-p-6}$.

From a 2-cube with linear complexity $2^{j+1} - (2^p + 2^q)$, we can have two 2-cubes with linear complexity $2^{j+1} - (2^q + 2^j)$.

Note that we can have 2^3 sequences, such as {0000 0011 0101 1111}, from the same sequence {0000 0000 0101 1111}. Furthermore, in the sequence {0000 0011 0101 1111}, all nonzero elements have alternate locations except the first two nonzero elements and the last two nonzero elements. Thus the number of these $s^{(n)}$ of type A can be given by

$$2^{4j-2q-p-6} \times 2 \times 2^2 \times (2^6)^{z-j-1} \times 2^3 \times 2^4 \times (2^8)^{n-z-1} = 2^{8n-2z-2j-2q-p-10}.$$

Similarly, we may derive the same counting formula of 2^n-periodic binary sequences of type B. Thus the total number of these $s^{(n)}$ can be given by

$$2^{8n-2z-2j-2q-p-9}.$$

(For sequence {0000 0011 0101 1111}, $n = 4, i_0 = 0, i = 1, j = 2$, $p = 0, q = 1, r = 3$, $x = 1, y = 2, z = 3$. With 2 bits change, it becomes a 2-cube and a 1-cube: {0000 0010 0101 0111}. With 4 bits change, it becomes a 3-cube: {0000 1111 0000 1111}. With 6 bits change, it becomes a 3-cube: {0101 0101 0101 0101}.)

2. In the case of $i_0 = p, i = x, q = j = y, r = z$. It is easy to show that there are two kinds of sequences $s^{(n)}$, illustrated by the following examples, meeting the condition of $L(s^{(n)}) = 2^n - 2^{i_0}$, $L_2(s^{(n)}) = 2^n - (2^i + 2^j)$, $L_4(s^{(n)}) = 2^n - (2^p + 2^q + 2^r)$ and $L_6(e) = 2^n - (2^x + 2^y + 2^z)$.

A) {0000 0011 0111 0111}; B) {0001 0001 0011 1111}, where $n = 4, i_0 = 0, i = 1, j = 2$, $p = 0, q = 2, r = 3$, $x = 1, y = 2, z = 3$.

From a 2-cube with linear complexity $2^{q+1} - (2^p + 2^q)$, we can have $2^{q-i-1} \times 2$ 2-cubes with linear complexity $2^{q+1} - (2^i + 2^q)$.

Thus the number of these $s^{(n)}$ of type A can be given by

$$2^{2q-p-2} \times 2^{q-i-1} \times 2 \times \frac{1}{2} \times (2^6)^{z-q-1} \times 2^3 \times 2^4 \times (2^8)^{n-z-1} = 2^{8n-2z-3q-p-i-10}.$$

Similarly, we may derive the same counting formula of 2^n-periodic binary sequences of type B. Thus the total number of these $s^{(n)}$ can be given by

$$2^{8n-2z-3q-p-i-9}.$$

(For sequence {0000 0011 0111 0111}, $n = 4, i_0 = 0, i = 1, j = 2$, $p = 0, q = 2, r = 3$, $x = 1, y = 2, z = 3$. With 2 bits change, it becomes a 2-cube and a 1-cube: {0000 0010 0101 0111}. With 4 bits change, it becomes a 3-cube: {0011 0011 0011 0011}. With 6 bits change, it becomes a 3-cube: {0101 0101 0101 0101}.)

3. In the case of $i_0 = p, i = x, q = y, j = r = z$. It is easy to show that there are two kinds of sequences $s^{(n)}$, illustrated by the following examples, meeting the condition of $L(s^{(n)}) = 2^n - 2^{i_0}$, $L_2(s^{(n)}) = 2^n - (2^i + 2^j)$, $L_4(s^{(n)}) = 2^n - (2^p + 2^q + 2^r)$ and $L_6(e) = 2^n - (2^x + 2^y + 2^z)$.

A) {0000 0111 0011 0111}; B) {0001 0011 1101 0011}, where $n = 4, i_0 = 0, i = 1, j = 3$, $p = 0, q = 2, r = 3$, $x = 1, y = 2, z = 3$.

The number of these $s^{(n)}$ of type A can be given by

$$2^{2j-p-2} \times 2^{j-i-1} \times 2 \times \frac{1}{2} \times 2^{j-q-1} \times 2^3 \times (2^8)^{n-j-1} = 2^{8n-4j-q-p-i-9}.$$

Similarly, we may derive the same counting formula of 2^n-periodic binary sequences of type B. Thus the total number of these $s^{(n)}$ can be given by

$$2^{8n-4j-q-p-i-8}.$$

(For sequence {0000 0111 0011 0111}, $n = 4, i_0 = 0, i = 1, j = 3$, $p = 0, q = 2, r = 3$, $x = 1, y = 2, z = 3$. With 2 bits change, it becomes two 2-cubes: {0010 0111 0010 0111}. With 4 bits change, it becomes a 3-cube: {0011 0011 0011 0011}. With 6 bits change, it becomes a 3-cube: {0101 0101 0101 0101}.)

4. In the case of $i_0 = q, i = p = x, j = y, r = z$. As $p < q < j$, the number of 2^j-periodic binary sequences $s^{(j)}$ with linear complexity $2^j - (2^q + 2^p)$ and $W_H(s^{(j)}) = 4$ is $2^{4j-2q-p-6}$.

From a 2-cube with linear complexity $2^{j+1} - (2^p + 2^q)$, we can have 2^2 2-cubes with linear complexity $2^{j+1} - (2^p + 2^j)$. Note that we only have 2^2 sequences, such as {0000 0110 0011 1111}, not being a 2-cube from the same sequence {0000 0000 0011 1111}.

Thus the number of these $s^{(n)}$ can be given by

$$2^{4j-2q-p-6} \times 2^2 \times 2^2 \times (2^6)^{z-j-1} \times 2^2 \times 2^4 \times (2^8)^{n-z-1} = 2^{8n-2z-2j-2q-p-10}.$$

(For sequence $\{0000\ 0011\ 0110\ 1111\}$, $n = 4, i_0 = 1, i = 0, j = 2$, $p = 0, q = 1, r = 3$, $x = 0, y = 2, z = 3$. With 2 bits change, it becomes a 2-cube and a 1-cube: $\{0000\ 0001\ 0110\ 0111\}$. With 4 bits change, it becomes a 3-cube: $\{0000\ 1111\ 0000\ 1111\}$. With 6 bits change, it can become a 3-cube: $\{0011\ 0011\ 0011\ 0011\}$.)

5. In the case of $i_0 = p, i = x, q < j = y < r < z$. As $p < q < j$, the number of 2^j-periodic binary sequences $s^{(j)}$ with linear complexity $2^j - (2^q + 2^p)$ and $W_H(s^{(j)}) = 4$ is $2^{4j-2q-p-6}$.

From a 2-cube with linear complexity $2^{j+1} - (2^p + 2^q)$, we have 2^2 2-cubes with linear complexity $2^{j+1} - (2^p + 2^j)$. Note that we can have 2^3 sequences, such as
$\{00000000\ 00000001\ 00010000\ 00111111\}$ and $\{00000000\ 00010000\ 00001000\ 00111111\}$, from the same sequence
$\{00000000\ 00000000\ 00000000\ 00111111\}$. Thus the number of these $s^{(n)}$ can be given by

$$2^{4j-2q-p-6} \times 2^2 \times 2^2 \times (2^6)^{r-j-1} \times 2^3 \times 2^5 \times (2^7)^{z-r-1} \times 2^6 \times (2^8)^{n-z-1} = 2^{8n-z-r-2j-2q-p-9}.$$

(For sequence $\{00000000\ 00000001\ 00000100\ 00111111\}$, $n = 5, i_0 = 0, i = 1, j = 2$, $p = 0, q = 1, r = 3$, $x = 0, y = 2, z = 4$. With 2 bits change, it becomes one 2-cube and two 1-cubes: $\{00000000\ 00000001\ 00000100\ 10101111\}$. With 4 bits change, it becomes a 3-cube: $\{00000000\ 00000000\ 00001111\ 00001111\}$. With 6 bits change, it becomes a 3-cube: $\{00000000\ 00110011\ 00000000\ 00110011\}$.)

6. In the case of $i_0 = p, i = x, q < j < y = r < z$. As $p < q < j$, the number of 2^{j+1}-periodic binary sequences $s^{(j+1)}$ with linear complexity $2^{j+1} - (2^q + 2^p)$ and $W_H(s^{(j+1)}) = 4$ is $2^{4j-2q-p-2}$.

From a 2-cube with linear complexity $2^{j+2} - (2^p + 2^q)$, we have two 2-cubes with linear complexity $2^{j+2} - (2^q + 2^(j+1))$. Note that we can have $2^{j-(p+1)} \times 2^{z+1-(j+1)}$ sequences, such as $\{00000000\ 00000001\ 10000101\ 00001111\}$ and $\{00000000\ 00000001\ 00000101\ 00101111\}$, from the same sequence $\{00000000\ 00000001\ 00000101\ 00001111\}$, where $p = 0, q = 1, j = 2, z = 4$. Thus the number of these $s^{(n)}$ can be given by

$$2^{4j-2q-p-2} \times 2 \times 2^2 \times 2^{j-(p+1)} \times 2^{j+2-(j+1)} \times (2^7)^{z-j-2} \times 2 \times 2^6 \times (2^8)^{n-z-1} = 2^{8n-z-2j-2q-2p-14}$$

(For sequence $\{00000000\ 00000100\ 10000101\ 00001111\}$, $n = 5, i_0 = 0, i = 1, j = 2$, $p = 0, q = 1, r = 3$, $x = 1, y = 3, z = 4$. With 2 bits change, it becomes one 2-cube and

two 1-cubes: {00000000 00000100 10100001 00001111}. With 4 bits change, it becomes a 3-cube: {00000000 00000000 00001111 00001111}. With 6 bits change, it becomes a 3-cube: {00000101 00000101 00000101 00000101}.)

This completes the proof. □

5.3 Summary

The k-error linear complexity profile of a periodic sequence was first defined by Stamp and Martin (1993). Based on the Games-Chan algorithm (Games and Chan, 1983) and the cube theory, a constructive approach has been presented to construct 2^n-periodic sequences with the given k-error linear complexity profile. Consequently, the complete counting formula of 2^n-periodic binary sequences has been derived with the given k-error linear complexity profile having descent points 1, 3, 5 and 7. The k-error linear complexity profile having descent points 2, 4, 6 and 8 has been also partially discussed. The proposed constructive approach can be used to construct 2^n-periodic binary sequences with the given linear complexity and k-error linear complexity.

We observed from the illustrative example in Appendix 10) that there are more sequences for large linear complexity and k-error linear complexity. However, there are some exceptions in the example. In fact, it is meaningful to investigate when the number of sequences can be achieved the maximum for some linear complexity and k-error linear complexity distribution. This would be our future research topic.

In future, we may further investigate the 2^n-periodic binary sequences with the k-error linear complexity profile of 5 or more descent points.

Chapter 6

Conclusions and Future Directions

The linear complexity and the k-error linear complexity of a sequence have been used as important security measures for key stream sequence strength in linear feedback shift register design. To further the study of the k-error linear complexity distribution for 2^n-periodic binary sequences, we began by proposing a **framework** in Chapter 2 as follows. Let $S = \{s|L(s) = c\}, E = \{e|W_H(e) \leq w\}, S + E = \{s + e|s \in S, e \in E\}$, where s is a sequence with linear complexity c, e is an error sequence with $W_H(e) \leq w$. We aimed to sieve sequences $s + e$ with $L_k(s + e) = c$ from $S + E$. This is the first fundamental contribution of this thesis. By a **divide and conquer** method of combinatorics, we investigated sequences with linear complexity 2^n, and sequences with linear complexity less than 2^n, separately. With our approach, the issue to study k-error linear complexity distribution for 2^n-periodic binary sequences becomes a combinatorial problem of these subsequences.

With our framework in Chapter 2 along with the sieve method, for $k = 2, 3, 4$, the complete counting functions on the k-error linear complexity of 2^n-periodic binary sequences with both *linear complexity* 2^n and *linear complexity less than* 2^n are characterized. We also obtained some partial results about the 5-error linear complexity of 2^n-periodic binary sequences. The first descent point (critical point) distribution of the k-error linear complexity for 2^n-periodic binary sequences was characterized completely in Chapter 2. We obtained the complete counting functions on the 2^m-error linear complexity of 2^n-periodic binary sequences with linear complexity $2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m})$, where $0 \leq i_1 < i_2 < \cdots < i_m < n$.

To address a sequence from different perspectives, we presented a new tool called the **Cube Theory** in Chapter 3. It is proved that a binary sequence with period 2^n can be decomposed into some disjoint cubes. Based on the Games-Chan Algorithm, we proposed **a standard cube decomposition** for any binary sequence with period 2^n. This is the second fundamental contribution of this thesis. With such cube decomposition theory, we are capable to construct sequences with the maximum stable k-error linear complexity. It was also proved that the maximum k-error linear complexity is $2^n - (2^l - 1)$ over all 2^n-periodic binary sequences, where $2^{l-1} \leq k < 2^l$ and $l < n$.

We then diverted our attention to the CELCS (critical error linear complexity spectrum) in Chapter 4. By the cube theory, a new approach to determining the CELCS for the k-error linear complexity distribution of 2^n-periodic binary sequences is developed via the sieve method and the Games-Chan algorithm. The **second descent point** distribution of the 3-error linear complexity, the second descent point distribution of the 4-error linear complexity and the **third descent point** distribution of the 5-error linear complexity for 2^n-periodic binary sequences were characterized completely. The k-error cube decomposition of 2^n-periodic binary sequences was also developed based on **the Cube Theory** of Chapter 3. As an extension of the work by Kurosawa *et al.* (2000), we derided the formulas to determine the second descent points and third descent points for the k-error linear complexity, respectively. This is the third important contribution of this thesis.

To conclude the thesis, we investigated k-error linear complexity profile in Chapter 5. Based on the Games-Chan algorithm and cube theory, a constructive approach was presented to **construct 2^n-periodic sequences with the given k-error linear complexity profile**. Consequently, the complete counting formula of 2^n-periodic binary sequences was derived with the given k-error linear complexity profile having descent points 1, 3, 5 and 7. The k-error linear complexity profile having descent points 2, 4, 6 and 8 was also partially discussed. The proposed constructive approach can be used to construct 2^n-periodic binary sequences with the given linear complexity and k-error linear complexity. This is the fourth important contribution of this thesis.

6.1 Future Study

With all of our proposed approaches and techniques, the study in this thesis opens many directions for periodic sequences with arbitrary period or periods of other forms. Despite all the significant achievements of this thesis, extensions to p^n-periodic sequences over F_p can also be considered. As a matter of fact, we have obtained some results for p^n-periodic sequences over F_p, where p is a prime number. However, due to the time limit, we did not cover them here. Specifically, we still have the following possible problems to study in near future.

- With our **Unified Approach** in Chapter 2, the issue to study k-error linear complexity distribution for 2^n-periodic binary sequences becomes a combinatorial problem of these subsequences. For $k \geq 5$, it is extremely complicated to calculate all the possible combinations of these subsequences. To develop some new techniques to address k-error linear complexity distribution for large k is a challenging future

work.

- To cope with a sequence from different perspectives, we present a new tool called the **Cube Theory** in Chapter 3. It is proved that a binary sequence with period 2^n can be decomposed into some disjoint cubes. We could further study how to construct sequences consisting of more than one cube and possessing both high linear complexity and k-error linear complexity. By using methods similar to that of the binary sequence, we may also study a sequence with period p^n over F_p, where p is a prime number.

- A new approach to determining the CELCS for the k-error linear complexity distribution of 2^n-periodic binary sequences was developed based on the cube theory in Chapter 4. Let $s^{(n)}$ be a 2^n-periodic binary sequence with linear complexity less then 2^n. Suppose that c_1, c_2 and c_3 are in the standard cube decomposition of sequence $s^{(n)}$ and $L(s^{(n)}) = L(c_1)$. $L_6(s^{(n)}) < L_4(s^{(n)}) < L_2(s^{(n)}) < L(s^{(n)})$ if and only if c_1 is one 1-cube and c_2 is one 2-cube or c_1, c_2 and c_3 are three 1-cubes. Similarly, we can compute the number of 2^n-periodic binary sequences $s^{(n)}$ with given $L(s^{(n)})$, $L_2(s^{(n)})$, $L_4(s^{(n)})$ and $L_6(s^{(n)})$. Accordingly, the solution to the complete counting functions of 2^n-periodic binary sequences with the prescribed 6-error linear complexity can be obtained. We expect that with the techniques proposed in Chapter 4, one can obtain other third and fourth descent point distributions of the k-error linear complexity for 2^n-periodic binary sequences.

- In Chapter 5, based on the Games-Chan algorithm (Games and Chan, 1983) and the cube theory, a constructive approach has been presented to construct 2^n-periodic sequences with the given k-error linear complexity profile. In future, we may investigate completely the k-error linear complexity profile having descent points 2, 4, 6 and 8. Furthermore, we also can consider the 2^n-periodic binary sequences with the k-error linear complexity profile of 5 or more descent points. Lastly, we believe that the proposed constructive approach can be used to construct 2^n-periodic binary sequences with the given linear complexity and k-error linear complexity.

Appendix A

Appendix for Chapter 5

In this appendix, we present some assertions once used in the proof of main results or some corollaries of the main results in Chapter 5. Of course, some of them have their own independent interests.

One can observe that every sequence $s^{(n)}$ has a unique standard cube decomposition by Algorithm 3.2.1 in Section 3.2, but sequence $s^{(n)}$ may has other cube decompositions as well.

1). 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 2-cube c_2 and one 1-cube c_3 by Algorithm 3.2.1 in Section 3.2, with $L(c_2) > L(c_3)$, $L_1(s^{(n)}) = 2^n - (2^i + 2^j), 0 \leq i < j < n$, $L_3(s^{(n)}) = 2^n - (2^p + 2^q + 2^r), 0 \leq p < q < r < n$, $L_5(s^{(n)}) = 2^n - (2^x + 2^y + 2^z), 0 \leq x < y < z < n$. Then $r < z$.

Proof. As $L_5(s^{(n)}) = 2^n - (2^x + 2^y + 2^z)$, thus $L_5(s^{(n)})$ is achieved by a 3-cube $\ddot{c}$. If $\ddot{c}$ includes 7 nonzero elements of $s^{(n)}$, then $L_5(s^{(n)}) = L_1(s^{(n)})$, which is a contradiction. If $\ddot{c}$ includes 6 nonzero elements of $s^{(n)}$, then $L_5(s^{(n)}) = L_3(s^{(n)})$, which is also a contradiction. So $\ddot{c}$ should only include 5 nonzero elements of $s^{(n)}$. Therefore, an edge length (based on Definition 2.3) is the distance (based on Definition 2.1) between two nonzero elements of $s^{(n)}$. Thus $L(c_3) = 2^n - 2^z$.

Suppose that $L_3(s^{(n)})$ is achieved by a 3-cube $\dot{c}$. So $\dot{c}$ should include 6 nonzero elements of $s^{(n)}$.

Let $T = \{\text{nonzero element } e | e \in \dot{c} \text{ and } e \in \ddot{c}\}$. So the number of nonzero elements in T is at least 4.

If the 4 nonzero elements in T does not constitute a 2-cube, then there are 3 distinct distance (based on Definition 2.1) among these nonzero elements in T. As a 3-cube only has 3 distinct edge length, thus $\dot{c}$ and $\ddot{c}$ have same edge length, which is followed by

$L_5(s^{(n)}) = L_3(s^{(n)})$. Therefore, the 4 nonzero elements in T does constitute a 2-cube.

If $r = z$, then there are 2 nonzero elements p_1, p_2 with distance z. As the 4 nonzero elements in T does constitute a 2-cube, so there are also other 2 nonzero elements p_3, p_4 with distance z, which contradicts the fact that c_3 is 1-cube.

This completes the proof. □

2). 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 2-cube c_2 and one 1-cube c_3 by Algorithm 3.2.1 in Section 3.2, with $L(c_2) > L(c_3)$, $L_1(s^{(n)}) = 2^n - (2^i + 2^j), 0 \leq i < j < n$, $L_3(s^{(n)}) = 2^n - (2^p + 2^q + 2^r), 0 \leq p < q < r < n$, $L_5(s^{(n)}) = 2^n - (2^x + 2^y + 2^z), 0 \leq x < y < z < n$. Then $i = x$ and $j = y$ can not be true at the same time.

Proof. As $L_5(s^{(n)}) = 2^n - (2^x + 2^y + 2^z)$, thus $L_5(s^{(n)})$ is achieved by a 3-cube $\ddot{c}$. If $\ddot{c}$ includes 7 nonzero elements of $s^{(n)}$, then $L_5(s^{(n)}) = L_1(s^{(n)})$, which is a contradiction. If $\ddot{c}$ includes 6 nonzero elements of $s^{(n)}$, then $L_5(s^{(n)}) = L_3(s^{(n)})$, which is also a contradiction. So $\ddot{c}$ should only include 5 nonzero elements of $s^{(n)}$.

In this case, we will prove the assertion by contradiction. Suppose that $i = x$ and $j = y$ are true at same time.

Suppose that the 0-cube c_1 includes a nonzero element e_1, the 2-cube c_2 includes 4 nonzero elements e_2, e_3, e_4, e_5, and the 1-cube c_3 includes 2 nonzero elements e_6, e_7. Thus $\ddot{c}$ should include e_6, e_7.

We will cope with the following 2 cases separately.

A) Suppose that $\ddot{c}$ also includes e_2, e_3, e_4.

Based on Algorithm 3.1.1 in Section 3.1, when the period of $s^{(n)}$ becomes 2^{z+1}, with $Left(s^{(z+1)}) \bigoplus Right(s^{(z+1)})$, e_6, e_7 will be removed, but e_2, e_3, e_4 will be remained. Otherwise, suppose that two nonzero elements of e_2, e_3, e_4 are removed. Then c_3 must be a 2-cube, which is a contradiction.

Thus, e_2, e_3, e_4 and e_7 constitute a 2-cube with linear complexity $2^z - (2^x + 2^y) = 2^z - (2^i + 2^j)$ (refer to Appendix 3) for the proof).

Suppose the distance of e_3, e_2 is 2^y. Then the distance of e_4 and e_7 is also 2^y.

As e_2, e_3, e_4, e_5 constitute a 2-cube with linear complexity $2^z - (2^x + 2^y) = 2^z - (2^i + 2^j)$, thus the distance of e_4 and e_5 is also 2^y. So the distance of e_5 and e_7 is 2^{y+1}.

Now we construct a 2-cube $\tilde{c}$ with linear complexity $2^n - (2^{y+1} + 2^z)$ and e_6, e_7, e_5, by adding a new nonzero element e_8, and changing e_1, e_2, e_3, e_4. As $2^n - (2^{y+1} + 2^z) < 2^n - (2^x + 2^y + 2^z)$, thus $L_5(s^{(n)}) = 2^n - (2^{y+1} + 2^z)$, which is a contradiction. Therefore, $i = x$ and $j = y$ can not be true at the same time in this case.

B) Suppose that $\ddot{c}$ also includes e_1, e_2, e_3.

Based on Algorithm 3.1.1 in Section 3.1, when the period of $s^{(n)}$ becomes 2^{z+1}, with $Left(s^{(z+1)}) \bigoplus Right(s^{(z+1)})$, e_6, e_7 will be removed, but e_1, e_2, e_3 will remain. Otherwise, suppose that two nonzero elements of e_1, e_2, e_3 are removed. Then c_3 must be a 2-cube, which is a contradiction.

As $i = x$ and $j = y$, the distance among e_1, e_2, e_3 must be 2^x and 2^y. In fact, e_1, e_2, e_3 and e_7 constitute a 2-cube with linear complexity $2^z - (2^x + 2^y) = 2^z - (2^i + 2^j)$ (refer to Appendix 3) for the proof).

Suppose the distance of e_1, e_2 is 2^y. Then the distance of e_3 and e_7 is 2^y.

As e_2, e_3, e_4, e_5 constitute a 2-cube with linear complexity $2^z - (2^x + 2^y) = 2^z - (2^i + 2^j)$, thus we can suppose that the distance of e_3 and e_5 is 2^y. So the distance of e_5 and e_7 is 2^{y+1}.

Now we construct a 2-cube $\tilde{c}$ with linear complexity $2^n - (2^{y+1} + 2^z)$ and e_6, e_7, e_5, by adding a new nonzero element e_8, and changing e_1, e_2, e_3, e_4. As $2^n - (2^{y+1} + 2^z) < 2^n - (2^x + 2^y + 2^z)$, thus $L_5(s^{(n)}) = 2^n - (2^{y+1} + 2^z)$, which is a contradiction. Therefore, $i = x$ and $j = y$ can not be true at the same time in this case.

In conclusion, the assertion is true in general. □

3). Let c be a 3-cube with linear complexity $2^n - (2^x + 2^y + 2^z), 0 \leq x < y < z < n$. Suppose that c incudes nonzero elements of $e_{i,j}, 1 \leq i \leq 2, 1 \leq j \leq 4$ and $e_{1,j}, 1 \leq j \leq 4$ constitute a 2-cube with linear complexity $2^n - (2^x + 2^y)$. Then $e_{i_j,j}, 1 \leq j \leq 4$ constitute a 2-cube with linear complexity $2^n - (2^x + 2^y)$, where i_j is 1 or 2.

Proof. From Definition 2.2, we know that $e_{2,j}, 1 \leq j \leq 4$ constitute a 2-cube with linear complexity $2^n - (2^x + 2^y)$.

Let $D(e_i, e_j)$ denote the distance of e_i and e_j. We only need to prove that $D(e_{1,j_1}, e_{1,j_2}) = D(e_{1,j_1}, e_{2,j_2})$ for $1 \leq j_1 \leq 4, 1 \leq j_2 \leq 4$.

As $D(e_{1,j_1}, e_{1,j_2}) | D(e_{1,j_2}, e_{2,j_2})$, where $D(e_{1,j_1}, e_{1,j_2}) = 2^x$ or 2^y, $D(e_{1,j_2}, e_{2,j_2}) = 2^z$, thus

$$D(e_{1,j_1}, e_{2,j_2}) \equiv (D(e_{1,j_1}, e_{1,j_2}) + D(e_{1,j_2}, e_{2,j_2})) \mod (D(e_{1,j_2}, e_{2,j_2})) = D(e_{1,j_1}, e_{1,j_2})$$

□

4). Assume that $s^{(n)}$ can be decomposed into one 0-cube c_1, and three 1-cubes c_2, c_3, c_4 by Algorithm 3.2.1 in Section 3.2, with $L_1(s^{(n)}) = 2^n - (2^i + 2^j), 0 \leq i < j < n$, $L_3(s^{(n)}) = 2^n - (2^p + 2^q), 0 \leq p < q < n$ and $L_5(s^{(n)}) = 2^n - (2^x + 2^y + 2^z), 0 \leq x < y < z < n$. Then $s^{(n)}$ includes a 2-cube.

Proof. As $L_5(s^{(n)}) = 2^n - (2^x + 2^y + 2^z)$, thus $L_5(s^{(n)})$ is achieved by a 3-cube $\ddot{c}$. If $\ddot{c}$ includes 7 nonzero elements of $s^{(n)}$, then $L_5(s^{(n)}) = L_1(s^{(n)})$, which is a contradiction. If $\ddot{c}$ includes 6 nonzero elements of $s^{(n)}$, then $L_5(s^{(n)}) = L_3(s^{(n)})$, which is also a contradiction. So $\ddot{c}$ should only include 5 nonzero elements of $s^{(n)}$.

Suppose that the 0-cube c_1 includes a nonzero element e_1, the 1-cubes c_2 and c_3 includes 4 nonzero elements e_2, e_3, e_4, e_5 and the 1-cube c_4 includes 2 nonzero elements e_6, e_7. Thus $\ddot{c}$ should include e_6, e_7.

Suppose that $\ddot{c}$ also includes e_1, e_2, e_3.

Based on Algorithm 3.1.1 in Section 3.1, when the period of $s^{(n)}$ becomes 2^{z+1}, with $Left(s^{(z+1)}) \bigoplus Right(s^{(z+1)})$, e_6, e_7 will be removed, but e_1, e_2, e_3 will be remained. Otherwise, suppose that two nonzero elements of e_1, e_2, e_3 are removed. Then c_4 must be a 2-cube, which is a contradiction.

Thus e_1, e_2, e_3 and e_6 constitute a 2-cube with linear complexity $2^n - (2^x + 2^y)$ (refer to Appendix 3) for the proof). □

5). Assume that $s^{(n)}$ can be decomposed into one 0-cube c_1, and three 1-cubes c_2, c_3, c_4 by Algorithm 3.2.1 in Section 3.2, $L_1(s^{(n)}) = 2^n - (2^i + 2^j), 0 \leq i < j < n$, $L_3(s^{(n)}) =$

$2^n - (2^p + 2^q), 0 \leq p < q < n$ and $L_5(s^{(n)}) = 2^n - (2^x + 2^y + 2^z), 0 \leq x < y < z < n$.

Suppose that the 0-cube c_1 includes a nonzero element e_1, the 1-cube c_2 includes 2 nonzero elements e_2, e_3, the 1-cube c_3 includes 2 nonzero elements e_4, e_5, and the 1-cube c_4 includes 2 nonzero elements e_6, e_7. Assume that e_1, e_2, e_3 and e_7 constitute a 2-cube with linear complexity $2^n - (2^x + 2^y)$. Then $i = x, j = y < q$, but $p \neq x$ and $p \neq y$.

Proof. Based on Algorithm 3.1.1 in Section 3.1, when the period of $s^{(n)}$ becomes 2^{z+1}, with
$Left(s^{(z+1)}) \bigoplus Right(s^{(z+1)})$, e_6, e_7 will be removed, but e_1, e_2, e_3 will be remained.

Suppose that $L(c_3) = 2^n - 2^q$. When the period of $s^{(n)}$ becomes 2^{q+1}, e_4, e_5 will be removed, so the distance among e_1, e_2, e_3 are $2^i = 2^x, 2^j = 2^y$ and $j < q$.

Let $D(e_i, e_j)$ denote the distance of e_i and e_j based on Definition 2.1. Suppose $D(e_1, e_2) = D(e_1, e_3) = 2^x$, $D(e_2, e_3) = 2^y$, where $x < y$.

We will prove $p \neq y$ by contradiction.

Suppose that $p = y$. Then there exits a nonzero element e in $\{e_1, e_2, e_3\}$, so that $D(e, e_4) = 2^y$.

If $D(e_2, e_4) = 2^y$, then $D(e_3, e_4) \geq 2^{y+1}$. So $p \geq y + 1$. The 2-cube with linear complexity $2^n - (2^p + 2^q)$ is achieved by changing e_1, e_2, and adding e_8, so that e_3, e_4, e_5 and e_8 constitute a 2-cube with linear complexity $2^n - (2^p + 2^q)$.

If $D(e_1, e_4) = 2^y$, then $D(e_4, e_3) = 2^x$. Thus e_1, e_2, e_3 and e_4 constitute a 2-cube with linear complexity $2^n - (2^x + 2^y)$. So by adding three new nonzero elements, e_1, e_2, e_3, e_4 and e_5 can constitute a 3-cube with linear complexity $2^n - (2^x + 2^y + 2^q)$, which contradicts to $L_3(s^{(n)}) = 2^n - (2^p + 2^q)$.

Thus we can conclude that $p \neq y$.

Similarly, we can prove that $p \neq x$. □

6). Assume that $s^{(n)}$ can be decomposed into one 0-cube c_1, and three 1-cubes c_2, c_3, c_4 by Algorithm 3.2.1 in Section 3.2, with $L_1(s^{(n)}) = 2^n - (2^i + 2^j), 0 \leq i < j < n$, $L_3(s^{(n)}) = 2^n - (2^p + 2^q), 0 \leq p < q < n$ and $L_5(s^{(n)}) = 2^n - (2^x + 2^y + 2^z), 0 \leq x < y < z < n$. Then

$L(c_2) = 2^n - 2^j$, $L(c_3) = 2^n - 2^q$ and $L(c_4) = 2^n - 2^z$.

Proof. Suppose that the 0-cube c_1 includes a nonzero element e_1, the 1-cube c_2 includes 2 nonzero elements e_2, e_3, the 1-cube c_3 includes 2 nonzero elements e_4, e_5, and the 1-cube c_4 includes 2 nonzero elements e_6, e_7.

Based on the result by Kurosawa *et al.* (2000), 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 $k_{\min} = 2^{W_H(2^n - L(s))}$. For a 1-cube c_2, $k_{\min} = 2$, which means that to further decrease the linear complexity of the 1-cube, we have to change 2 elements. So the $L_1(s^{(n)})$ is achieved by a 2-cube, which is composed of e_1, e_2, e_3 and a new nonzero element e_8. From Algorithm 3.2.1 in Section 3.2, the distance of e_2, e_3 is greater than both the distance of e_1, e_2 and the distance of e_1, e_3. As $L_1(s^{(n)}) = 2^n - (2^i + 2^j), 0 \leq i < j < n$, thus the distance of e_2, e_3 is 2^j, which is followed by $L(c_2) = 2^n - 2^j$.

Let 2^d be the maximum of $\{D(e_i, e_j) | 1 \leq i \leq 3, 4 \leq j \leq 5\}$, where $D(e_i, e_j)$ denotes the distance of e_i and e_j based on Definition 2.1. Without loss of generality, suppose that $D(e_1, e_4) = 2^d$. Then $L_3(s^{(n)})$ is achieved by a 2-cube, which is composed of e_1, e_4, e_5 and a new nonzero element e_9. From Algorithm 3.2.1 in Section 3.2, the distance of e_4, e_5 is greater than both the distance of e_1, e_4 and the distance of e_1, e_5. As $L_3(s^{(n)}) = 2^n - (2^p + 2^q), 0 \leq p < q < n$, thus the distance of e_4, e_5 is 2^q, which is followed by $L(c_3) = 2^n - 2^q$.

Suppose that $L(c_4) = 2^n - 2^{z'}$. As $L_5(s^{(n)}) = 2^n - (2^x + 2^y + 2^z) \leq L(c_4)$, thus $z \geq z'$.

Refer to Appendix 4), we know that $L_5(s^{(n)})$ is achieved by a 3-cube $\ddot{c}$ and $\ddot{c}$ should include 5 nonzero elements of $s^{(n)}$, thus $z \leq z'$. Therefore, $z = z'$. □

7). Assume that $s^{(n)}$ can be decomposed into one 0-cube c_1, and three 1-cubes c_2, c_3, c_4 by Algorithm 3.2.1 in Section 3.2, $L_1(s^{(n)}) = 2^n - (2^i + 2^j), 0 \leq i < j < n$, with $L_3(s^{(n)}) = 2^n - (2^p + 2^q), 0 \leq p < q < n$ and $L_5(s^{(n)}) = 2^n - (2^x + 2^y + 2^z), 0 \leq x < y < z < n$. Further suppose that the 0-cube c_1 includes a nonzero element e_1, the 1-cubes c_2 and c_3 includes 4 nonzero elements e_2, e_3, e_4, e_5, and the 1-cube c_4 includes 2 nonzero elements e_6, e_7. Based on Appendix 4), we can assume that e_1, e_2, e_3 and e_7 constitute a 2-cube with linear complexity $2^n - (2^x + 2^y)$. Now by Algorithm 3.2.1 in Section 3.2, if the second removed two nonzero elements are e_3, e_4, then we only need to consider 3 cases: $i = x < j < p = y < q$, $i < j = x < p = y < q$, and $i < p = x < j = y < q$. Other cases

are covered by the case in which the removed two nonzero elements in the second time at Step 2 of Algorithm 3.2.1 in Section 3.2 are e_4, e_5.

Proof. There are two cases: $D(e_3, e_7) = 2^x$ or 2^y.

A) Suppose that $D(e_3, e_7) = 2^x$. Note that that e_1, e_2, e_3 and e_7 constitute a 2-cube with linear complexity $2^n - (2^x + 2^y)$. Without loss of generality, suppose that $D(e_3, e_1) = 2^y$. Then $D(e_1, e_2) = 2^x$, $D(e_2, e_7) = 2^y$ and $D(e_3, e_2) = 2^x$

Refer to Appendix 6), $L_3(s^{(n)})$ is determined by e_1, e_2, e_3, e_4, e_5.

If $D(e_3, e_5) < 2^y$, then $D(e_4, e_5) \equiv D(e_4, e_3) + D(e_3, e_5) \equiv 2^q + D(e_3, e_5) \mod (2^q) = D(e_3, e_5) < 2^y$. Thus $L_3(s^{(n)}) = 2^n - (2^y + 2^q)$. So $p = y$.

$L_1(s^{(n)})$ is determined by e_1, e_2, e_5. So $i = x$ or $j = x$. There are two cases: $i = x < j < p = y < q$, $i < j = x < p = y < q$.

If $D(e_3, e_5) = 2^p > 2^y$, then $D(e_5, e_7) \equiv D(e_5, e_3) + D(e_3, e_7) \equiv 2^p + 2^x \equiv 2^x \mod (2^p)$, $D(e_5, e_1) \equiv D(e_5, e_3) + D(e_3, e_1) \equiv 2^p + 2^y \equiv 2^y \mod (2^p)$, $D(e_5, e_2) \equiv D(e_5, e_3) + D(e_3, e_2) \equiv 2^p + 2^x \equiv 2^x \mod (2^p)$.

Thus e_1, e_2, e_5 and e_7 constitute a 2-cube with linear complexity $2^n - (2^x + 2^y)$. This is the case that $i = x < j = y < p < q < z$, which is already covered by the case that the second removed two nonzero elements are e_4, e_5.

B) Suppose that $D(e_3, e_7) = 2^y$.

Without loss of generality, suppose that $D(e_3, e_1) = 2^x$. Then $D(e_1, e_2) = 2^y$, $D(e_2, e_7) = 2^x$ and $D(e_3, e_2) = 2^x$

Refer to Appendix 6), $L_3(s^{(n)})$ is determined by e_1, e_2, e_3, e_4, e_5.

If $D(e_3, e_5) < 2^x$, then $D(e_4, e_5) \equiv D(e_4, e_3) + D(e_3, e_5) \equiv 2^q + D(e_3, e_5) \mod (2^q) = D(e_3, e_5) < 2^x$. Thus $L_3(s^{(n)}) = 2^n - (2^x + 2^q)$. So $p = x$.

$L_1(s^{(n)})$ is determined by e_1, e_2, e_5. So $j = y$. Thus $i < p = x < j = y < q$.

If $2^x < D(e_3, e_5) = 2^p < 2^y$, then $D(e_4, e_5) \equiv D(e_4, e_3) + D(e_3, e_5) \equiv 2^q + 2^p \mod (2^q) = 2^p$, $D(e_2, e_5) \equiv D(e_2, e_3) + D(e_3, e_5) \equiv 2^x + 2^p \mod (2^p) = 2^x$, Thus $L_3(s^{(n)}) = 2^n - (2^p +$

2^q).

$L_1(s^{(n)})$ is determined by e_1, e_2, e_5. As $D(e_1, e_2) = 2^y$, so $i = x, j = y$. Thus $i = x < p < j = y < q < z$, which is already covered by the case that the second removed two nonzero elements are e_4, e_5.

If $D(e_3, e_5) = 2^p > 2^y$, then $D(e_5, e_7) \equiv D(e_5, e_3) + D(e_3, e_7) \equiv 2^p + 2^y \equiv 2^y \mod (2^p)$, $D(e_5, e_1) \equiv D(e_5, e_3) + D(e_3, e_1) \equiv 2^p + 2^x \equiv 2^x \mod (2^p)$, $D(e_5, e_2) \equiv D(e_5, e_3) + D(e_3, e_2) \equiv 2^p + 2^x \equiv 2^x \mod (2^p)$.

Thus e_1, e_2, e_5 and e_7 constitute a 2-cube with linear complexity $2^n - (2^x + 2^y)$. This is the case that $i = x < j = y < p < q < z$, which is already covered by the case that the second removed two nonzero elements are e_4, e_5. □

8). Assume that $s^{(n)}$ can be decomposed into one 0-cube c_1, and three 1-cubes c_2, c_3, c_4 by Algorithm 3.2.1 in Section 3.2, with $L_1(s^{(n)}) = 2^n - (2^i + 2^j), 0 \le i < j < n$, $L_3(s^{(n)}) = 2^n - (2^p + 2^q + 2^r), 0 \le p < q < r < n$ and $L_5(s^{(n)}) = 2^n - (2^x + 2^y + 2^z), 0 \le x < y < n$. Then $y = r$.

Proof. It is obvious that $L(c_2) = 2^n - 2^j, L(c_3) = 2^n - 2^r, L(c_4) = 2^n - 2^z$.

Suppose that the 0-cube c_1 includes a nonzero element e_1, the 1-cubes c_2 and c_3 includes 4 nonzero elements e_2, e_3, e_4, e_5 and the 1-cube c_4 includes 2 nonzero elements e_6, e_7.

Note that $L_3(s^{(n)}) = 2^n - (2^p + 2^q + 2^r)$ is achieved with a 3-cube $\dot{c}$ by changing e_6 or e_7, and adding two new nonzero elements.

Thus there are at least two pairs of nonzero elements in e_1, e_2, e_3, e_4, e_5 and e_6, so that distance of each pair of nonzero elements is 2^r.

Without loss of generality, suppose that $D(e_4, e_5) = 2^r$ and $D(e_1, e_6) = 2^r$. As c_3 is a 1-cube, thus one nonzero element in e_1, e_4, e_5 and e_6 and e_7 must constitute a 1-cube c_4 with linear complexity $2^n - 2^z$.

Suppose that $D(e_4, e_1) = 2^p$. Then we can construct a 3-cube $\ddot{c}$ with linear complexity $2^n - (2^p + 2^r + 2^z)$ by changing e_2 and e_3, and adding three new nonzero elements. As $2^n - (2^p + 2^r + 2^z) \ge 2^n - (2^x + 2^y + 2^z)$, so $r \le y$.

Note that e_1, e_2, e_3 and e_6 constitute a 2-cube with linear complexity $2^n - (2^x + 2^y)$ (refer to Appendix 3) for the proof), thus $y \leq r$. So $y = r$. □

9). Suppose that $s^{(n)}$ can be decomposed into one 0-cube c_1 with one nonzero element e_1, one 1-cube c_2 with two nonzero elements e_2, e_3) and one 2-cube c_3 with four nonzero elements e_4, e_5, e_6, e_7. Also $s^{(n)}$ has linear complexity $2^n - (2^u + 2^v), u < v$ from Algorithm 3.2.1 in Section 3.2, with $L(c_2) > L(c_3)$. Further assume that $L_1(s^{(n)}) = 2^n - (2^i + 2^j), 0 \leq i < j < n$, $L_3(s^{(n)}) = 2^n - (2^p + 2^q), 0 \leq p < q < n$, $L_5(s^{(n)}) = 2^n - (2^x + 2^y + 2^z), 0 \leq x < y < z < n$. If $s^{(n)}$ contains two distinct 2-cubes, then there are only 4 possible cases as follows: 1. $i = x > p, j = y, q = z$, 2. $i = x < p, j = y, q = z$, 3. $p = x, j = y, q = z$, 4. $j = x, p = y, q = z$.

Proof. Assume that $L_1(s^{(n)}) = 2^n - (2^i + 2^j), 0 \leq i < j < n$, $L_3(s^{(n)}) = 2^n - (2^p + 2^q), 0 \leq p < q < n$, $L_5(s^{(n)}) = 2^n - (2^x + 2^y + 2^z), 0 \leq x < y < z < n$. We know that the distance among nonzero elements e_1, e_2, e_3 is neither u nor v. $L_3(s^{(n)})$ is achieved by c_3, so $L_3(s^{(n)}) = 2^n - (2^p + 2^q) = 2^n - (2^u + 2^v)$, thus $q = z = v$.

Assume that the 2-cube c_4 is different from 2-cube c_3. From Algorithm 3.2.1 in Section 3.2, $L(c_4) < L(c_3)$. Thus $L_1(s^{(n)})$ is achieved by a 2-cube containing nonzero elements e_1, e_2, e_3, and $2^i, 2^j$ are the distance among nonzero elements e_1, e_2, e_3.

Let S_j be the intersection of the nonzero elements of c_3 and the nonzero elements of c_4. If S_j contains two nonzero elements e_8, e_9, then the distance of e_8, e_9 is u or v. It means that the distance of two nonzero elements of e_1, e_2, e_3 is u or v, which is a contradiction.

So S_j contains only one nonzero elements e_8. Thus e_1, e_2, e_3 and e_8 constitute the 2-cube c_4 with linear complexity $2^n - (2^i + 2^j)$.

If $L_5(s^{(n)})$ is achieved by a 3-cube containing c_4, then $\{i, j\} \subset \{x, y, z\}$. Thus $x = i, y = j$. So we have the following cases. 1. $i = x > p, j = y, q = z$, 2. $i = x < p, j = y, q = z$.

If $L_5(s^{(n)})$ is achieved by a 3-cube containing c_3, then $\{p, q\} \subset \{x, y, z\}$ and x or y must be $\max\{i, j\} = j$. So we have the cases of 3. $p = x, j = y, q = z$, 4. $j = x, p = y, q = z$. □

10). The complete 2^n-periodic binary sequence distribution with the given k-error linear complexity profile of $0 = L_7(s^{(n)}) < L_5(s^{(n)}) < L_3(s^{(n)}) < L_1(s^{(n)}) < L(s^{(n)}) = 2^n$ for $n = 5$.

Table 1. The sequence distribution for $n = 5$

L_1	L_3	L_5	Number of sequences	L_1	L_3	L_5	Number of sequences
12	10	6	128	23	14	7	2048
12	11	7	256	23	14	10	8192
14	6	4	128	23	14	11	8192
14	10	4	256	23	19	4	2048
14	13	7	512	23	19	11	4096
14	13	11	1024	23	19	14	16384
15	7	4	256	23	19	18	8192
15	7	6	512	23	21	6	4096
15	11	4	512	23	21	12	24576
15	11	10	1024	23	21	13	16384
15	13	6	1024	23	21	18	16384
15	13	10	2048	26	8	4	512
20	14	4	512	26	8	7	2048
20	14	13	2048	26	10	4	1024
20	15	4	1024	26	10	6	2048
20	15	13	4096	26	15	7	12288
20	18	6	512	26	15	10	8192
20	18	10	1024	26	18	4	2048
20	18	15	4096	26	18	6	4096
20	19	7	1024	26	18	15	16384
20	19	11	2048	26	23	7	24576
20	19	14	8192	26	23	10	16384
22	6	4	256	26	23	11	16384
22	12	4	512	26	23	13	32768
22	12	6	512	26	23	18	32768
22	12	11	2048	26	25	8	40960
22	15	6	2048	26	25	11	16384
22	15	11	8192	26	25	13	32768
22	18	4	1024	26	25	19	32768
22	18	10	2048	26	25	21	65536
22	18	15	8192	27	8	4	1024
22	21	7	2048	27	8	6	4096
22	21	12	12288	27	11	4	2048
22	21	13	8192	27	11	7	4096
22	21	19	8192	27	11	10	4096
23	7	4	512	27	14	6	12288
23	7	6	1024	27	14	7	12288
23	12	4	1024	27	14	10	8192
23	12	7	1024	27	14	11	8192
23	12	10	4096	27	19	4	4096
23	14	6	2048	27	19	7	8192

L_1	L_3	L_5	Number of sequences
27	19	14	32768
27	19	18	16384
27	22	6	24576
27	22	7	24576
27	22	10	16384
27	22	11	49152
27	22	13	65536
27	22	18	32768
27	22	19	32768
27	25	8	81920
27	25	10	32768
27	25	13	65536
27	25	18	65536
27	25	21	131072
29	8	4	6144
29	8	6	4096
29	12	4	12288
29	12	6	8192
29	12	7	16384
29	12	10	8192
29	13	6	8192
29	13	7	16384
29	13	10	16384
29	13	11	32768
29	20	4	24576
29	20	6	16384
29	20	7	32768
29	20	10	32768
29	20	11	65536
29	20	13	98304
29	20	18	32768
29	21	6	16384
29	21	7	32768
29	21	12	131072
29	21	18	65536
29	21	19	131072
29	25	8	163840
29	25	10	65536
29	25	11	131072
29	25	18	131072
29	25	19	262144

Here are some illustrative examples of computation.

For $n = 5, L_1(s^{(n)}) = 12 = 32 - (4 + 16)$, $L_3(s^{(n)}) = 10 = 32 - (2 + 4 + 16)$, $L_5(s^{(n)}) = 6 = 32 - (2 + 8 + 16)$. We know that $j = r = z = 4, i = q = 2, p = x = 1, y = 3$, which is the case of $i = q < y, j = r = z, p = x$. From Theorem 5.1.3 i)., the number of sequences $s^{(n)}$ is $2^{7n-3j-i-x-y-10} = 2^7 = 128$.

For $n = 5, L_1(s^{(n)}) = 26 = 32 - (2 + 4)$, $L_3(s^{(n)}) = 8 = 32 - (8 + 16)$, $L_5(s^{(n)}) = 4 = 32 - (4 + 8 + 16)$. We know that $j = x = 2, p = y = 3, q = z = 4, i = 1$, which is the case of $j = x, p = y, q = z$. From Theorem 5.1.3 ii)., the number of sequences $s^{(n)}$ is $2^{7n-2j-i-2z-y-10} = 2^9 = 512$.

For $n = 5, L_1(s^{(n)}) = 29 = 32 - (1 + 2)$, $L_3(s^{(n)}) = 25 = 32 - (1 + 2 + 4)$, $L_5(s^{(n)}) = 19 = 32 - (1 + 4 + 8)$. We know that $i = p = x = 0, j = q = 1, r = y = 2, z = 3$, which is the case of $i = p = x < j = q < r = y < z$. From Theorem 5.1.1 iv)., the number of sequences $s^{(n)}$ is $2^{7n-z-2r-2j-i-8} = 2^{18} = 262144$.

Bibliography

Chang, Z. and Wang, X. (2013). On the first and second critical error linear complexity of binary 2^n-periodic sequences. *Chinese Journal of Electronics*, **22**(1), 1–6.

Ding, C. (1990). Lower bounds on the weight complexities of cascaded binary sequences. In *International Conference on Cryptology*, pages 39–43. Springer.

Ding, C., Xiao, G., and Shan, W. (1991). *The stability theory of stream ciphers*, volume 561. Springer Science & Business Media.

Dohmen, K. (1999). An improvement of the inclusion-exclusion principle. *Archiv der Mathematik*, **72**(4), 298–303.

Etzion, T., Kalouptsidis, N., Kolokotronis, N., Limniotis, K., and Paterson, K. G. (2009). Properties of the error linear complexity spectrum. *IEEE Transactions on Information Theory*, **55**(10), 4681–4686.

Fu, F.-W., Niederreiter, H., and Su, M. (2006). The characterization of 2^n-periodic binary sequences with fixed 1-error linear complexity. In *International Conference on Sequences and Their Applications*, pages 88–103. Springer.

Games, R. and Chan, A. (1983). A fast algorithm for determining the complexity of a binary sequence with period 2^n. *IEEE Transactions on Information Theory*, **29**(1), 144–146.

Hu, H.-G. and Feng, D.-G. (2005). Periodic sequences with very large 1-error linear complexity over F(q). *Ruan Jian Xue Bao(J. Softw.)*, **16**(5), 940–945.

Kaida, T., Uehara, S., and Imamura, K. (1999). An algorithm for the k-error linear complexity of sequences over gf (p m) with period pn, p a prime. *Information and Computation*, **151**(1), 134–147.

Kavuluru, R. (2008). 2^n-periodic binary sequences with fixed k-error linear complexity for $k = 2$ or 3. In *International Conference on Sequences and Their Applications*, pages 252–265. Springer.

Kavuluru, R. (2009). Characterization of 2^n-periodic binary sequences with fixed 2-error or 3-error linear complexity. *Designs, Codes and Cryptography*, **53**(2), 75–97.

Kurosawa, K., Sato, F., Sakata, T., and Kishimoto, W. (2000). A relationship between linear complexity and k-error linear complexity. *IEEE Transactions on Information Theory*, **46**(2), 694–698.

Lauder, A. G. and Paterson, K. G. (2003). Computing the error linear complexity spectrum of a binary sequence of period 2^n. *IEEE Transactions on Information Theory*, **49**(1), 273–280.

Massey, J. (1969). Shift-register synthesis and bch decoding. *IEEE transactions on Information Theory*, **15**(1), 122–127.

Meidl, W. (2004). How many bits have to be changed to decrease the linear complexity? *Designs, Codes and Cryptography*, **33**(2), 109–122.

Meidl, W. (2005). On the stability of 2^n-periodic binary sequences. *IEEE Transactions on Information Theory*, **51**(3), 1151–1155.

Meidl, W. and Niederreiter, H. (2002). Linear complexity, k-error linear complexity, and the discrete fourier transform. *Journal of Complexity*, **18**(1), 87–103.

Menezes, A. J., Van Oorschot, P. C., and Vanstone, S. A. (1996). *Handbook of applied cryptography*. CRC press.

Niu, Z., Li, Z., Li, Z., and Xin, M. (2013). The research and analysis of the excellent 2^n periodic binary sequence based on cat swarm optimization. *Journal of Electronics and Information Technology (China)*, **35**(6), 1365–1370.

Niu, Z., Ye, F., Xin, M., and Wang, C. (2014). Generation and analysis of the excellent 2^n-periodic binary sequences. *Journal of Xidian University (China)*, **41**(1), 130–134.

Paar, I. C. and Pelzl, I. J. (2010). Stream ciphers. In *Understanding Cryptography*, pages 29–54. Springer.

Pan, W., Bao, Z., Lin, D., and Liu, F. (2016). The linear complexity and 2-error linear complexity distribution of 2^n-periodic binary sequences with fixed hamming weight. In *International Conference on Information and Communications Security*, pages l07–123. Springer.

Pi, F. and Qi, W. (2011). The 4-error linear complexity of binary periodic sequences. *Acta Electronica Sinica (in Chinese)*, **39**(12), 2914–2920.

Rueppel, R. A. (2012). *Analysis and design of stream ciphers*. Springer Science & Business Media.

Salagean, A. (2005). On the computation of the linear complexity and the k-error linear complexity of binary sequences with period a power of two. *IEEE transactions on information theory*, **51**(3), 1145–1150.

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

Zhou, J. (2011). On the k-error linear complexity of sequences with period $2p^n$ over GF(q). *Designs, Codes and Cryptography*, **58**(3), 279–296.

Zhou, J. (2012). A counterexample concerning the 3-error linear complexity of 2^n-periodic binary sequences. *Designs, Codes and Cryptography*, **64**(3), 285–286.

Zhou, J. and Liu, W. (2014). The k-error linear complexity distribution for 2^n-periodic binary sequences. *Designs, codes and cryptography*, **73**(1), 55–75.

Zhou, J., Liu, W., and Zhou, G. (2013). Cube theory and stable k-error linear complexity for periodic sequences. In *International Conference on Information Security and Cryptology*, pages 70–85. Springer.

Zhou, J., Liu, W., and Wang, X. (2015a). Characterization of the third descent points for the k-error linear complexity of 2^n-periodic binary sequences. In *International Conference on Information and Communications Security*, pages 169–183. Springer.

Zhou, J., Liu, W., and Wang, X. (2015b). The cube theory for 2^n-periodic binary sequences. In *2015 9th International Conference on Future Generation Communication and Networking (FGCN)*, pages 1–4. IEEE.

Zhou, J., Liu, W., and Wang, X. (2016). Cube theory and k-error linear complexity profile. *International Journal of Security and Its Applications*, **10**(7), 169–184.

Zhu, F. and Qi, W. (2007). The 2-error linear complexity of 2^n-periodic binary sequences with linear complexity $2^n - 1$. *Journal of Electronics (China)*, **24**(3), 390–395.