STRUCTURE ANALYSIS ON THE $k$-ERROR LINEAR
COMPLEXITY FOR $2^n$-PERIODIC BINARY SEQUENCES

JIANQIN ZHOU
Department of Computing, Curtin University
Perth, WA 6102, Australia
and
School of Computer Science, Anhui Univ. of Technology
Ma’anshan 243032, China

WANQUAN LIU
Department of Computing, Curtin University
Perth, WA 6102, Australia

XIFENG WANG
School of Computer Science, Anhui Univ. of Technology
Ma’anshan 243032, China

Abstract. In this paper, in order to characterize the critical error linear complexity spectrum (CELCS) for $2^n$-periodic binary sequences, we first propose a decomposition based on the cube theory. Based on the proposed $k$-error cube decomposition, and the famous inclusion-exclusion principle, we obtain the complete characterization of the $i$th descent point (critical point) of the $k$-error linear complexity for $i = 2, 3$. 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.

1. Introduction. 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 $s$. According to the Berlekamp-Massey algorithm [9], if the linear complexity of a sequence $s$ is $L(s)$, and $2L(s)$ consecutive elements of the sequence are known, then the whole sequence can be determined. So the linear complexity of a key sequence should be large enough to resist known plain text attack. As a measure on the stability of linear complexity for sequences, the weight complexity and sphere complexity were defined in the monograph by Ding, Xiao and Shan in 1991 [2]. Similarly, Stamp and Martin [13] 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 elements of the sequence are changed within one period.

The reason why people study the stability of linear complexity is that a small number of element changes may lead to a sharp decline of linear complexity. How many elements have to be changed to reduce the linear complexity? Kurosawa et al. in [7] introduced the concept of minimum error(s) to deal with the problem, and defined it as the minimum number $k$ for which the $k$-error linear complexity is strictly less than the linear complexity of sequence $s$, which is determined by $2^{W_H(2^n-L(s))}$, where $W_H(a)$ denotes the Hamming weight of the binary representation of an integer $a$. In [10], 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. In [14], 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.

In another research direction, Rueppel [12] 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 [11] 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 [18] 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. [4] 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. The complete counting functions for the number of $2^n$-periodic binary sequences with the 3-error linear complexity are characterized recently in [15].

The CELCS (critical error linear complexity spectrum) is studied in [8, 3]. 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 $k' > k$. In fact they are the points where a decrease occurs for the $k$-error linear complexity, and thus are called descent points.

Kurosawa et al. in [7] gave an important result about the first descent point of the $k$-error linear complexity. Due to its difficulty, the second descent point is rarely investigated in literature. In this paper, we propose a $k$-error cube decomposition for $2^n$-periodic binary sequences to investigate the $i$th descent point of the $k$-error linear complexity. By applying the famous inclusion-exclusion principle in combinatorics, we obtain the complete characterization of the $i$th descent point of the $k$-error linear complexity for $i = 2, 3$.

One of our main results is that there exists a $k$-error cube decomposition for a given $2^n$-periodic binary sequence. With a given series of linear complexity values $L(c^{(0)}), L(c^{(1)}), L(c^{(2)}), \ldots, L(c^{(m)})$, our focus is how to construct a sequence $s^{(n)}$ with the right $k$-error cube decomposition $s^{(n)} = c^{(0)} + c^{(1)} + c^{(2)} + \cdots + c^{(m)}$, so that $L(c^{(i)}) = L^{(i)}(s^{(n)})$, where $L^{(i)}(s^{(n)})$ is the $k$-error linear complexity of the $i$th descent point for $s^{(n)}$.

In previous research, investigators focus on the linear complexity and $k$-error complexity for a given sequence. In this paper, the motivation of this paper is to construct $2^n$-periodic binary sequences with the given linear complexity and $k$-error linear complexity (or CELCS), and this is a more challenging problem with broad applications.
The rest of this paper is organized as follows. In Section II, we first give an outline about our main approach for characterizing CELCS for $2^n$-periodic binary sequences. Also some preliminary results are presented. In Section III, the $k$-error cube decomposition for $2^n$-periodic binary sequences is proposed to investigate the $i$th descent point of the $k$-error linear complexity. By applying the famous inclusion-exclusion principle, the complete characterization of the $i$th descent point of the $k$-error linear complexity is presented for $i = 2, 3$. Concluding remarks are given in Section IV.

2. Preliminaries. In this section we first give some preliminary results which will be used in the sequel. At the same time an outline about the proposed constructive approach is presented for characterizing CELCS for the $k$-error linear complexity distribution of $2^n$-periodic binary sequences.

Let $x = (x_1, x_2, \cdots, x_n)$ and $y = (y_1, y_2, \cdots, y_n)$ be vectors over $GF(q)$. Then define $x + y = (x_1 + y_1, x_2 + y_2, \cdots, x_n + y_n)$. 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 per period of $s$, denoted by $W_H(s)$. Let $s^N$ be one period of $s$. If $N = 2^n$, $s^N$ is also denoted as $s^{(n)}$. The absolute distance of two elements is defined as the difference of their indexes.

The linear complexity of a $2^n$-periodic binary sequence $s$ can be recursively computed by the Games-Chan algorithm [5] stated as follows.

Algorithm 2.1

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

Output: $L(s) = c$.

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

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

Repeat Step 1 and Step 2 recursively until one element is left.

Step 3. $s = (a)$, if $a = 1$ then $c = c + 1$, else $c = c + 0$.

The following two lemmas are well known results on $2^n$-periodic binary sequences. Please refer to [11, 18, 15] for details.

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

Lemma 2.2. Let $s_1$ and $s_2$ be two binary sequences with period $2^n$. 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. By Lemma 2.2, the linear complexity of the binary sequence, in which elements at exactly those $k$ positions are all nonzero, must be $L(s)$. Therefore, for the computation of the $k$-error linear complexity, we only need to find the binary sequence whose Hamming weight is the minimum and its linear complexity is $L(s)$.

Based on Games-Chan algorithm, the following lemma is given in [11].

Lemma 2.3. 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 $\varphi_n$ from $F_2^{2^n}$ to $F_2^{2^{n-1}}$ is defined as
\[
\varphi_n(s^{(n)}) = \varphi_n((s_0, s_1, s_2, \cdots, s_{2^n-1})) \\
= (s_0 + s_{2^n-1}, s_1 + s_{2^n-1+1}, \cdots, s_{2^n-1-1} + s_{2^n-1})
\]

Let \(W_H(v)\) denote the Hamming weight of a vector \(v\). Then the mapping \(\varphi_n\) has the following properties.

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

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

3) The set
\[\varphi_n^{-1}(s^{(n)}) = \{v \in F_2^{n+1} | \varphi_n(v) = s^{(n)}\}\]
of the preimage of \(s^{(n)}\) has cardinality \(2^n\).

Rueppel [12] presented the following preliminary result on the number of sequences with a given linear complexity.

**Lemma 2.4.** The number \(N(L)\) of \(2^n\)-periodic binary sequences with linear complexity \(L, 0 \leq L \leq 2^n\), is given by \(N(L) = \begin{cases} 1, & L = 0 \\ 2L-1, & 1 \leq L \leq 2^n \end{cases}\)

Based on algebraic and combinatorial methods, Fu et al. [4] 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. Meidl [11] characterized the complete counting functions on the 1-error linear complexity of \(2^n\)-periodic binary sequences with linear complexity \(2^n\). Zhu and Qi [18] gave the complete counting functions on the 2-error linear complexity of \(2^n\)-periodic binary sequences with linear complexity \(2^n - 1\).

In this paper, in order to characterize CELCS (critical error linear complexity spectrum), we will use the Cube Theory recently introduced in [16, 17]. Cube theory and some related results are presented next for completeness.

Suppose that the position difference of two non-zero elements of a sequence \(s\) is \((2x + 1)2^y\), where \(x\) and \(y\) are non-negative integers. From Algorithm 2.1, only in the \((n - y)\)th step, the sequence length is \(2^{y+1}\), so the two non-zero elements must be in the left and right half of the sequence respectively, thus they can be removed or reduce to one non-zero element in consequence operation. Therefore we have the following definitions.

**Definition 2.5.** ([16, 17]) Suppose that the position difference of two non-zero elements of a sequence \(s\) is \((2x + 1)2^y\), where both \(x\) and \(y\) are non-negative integers. Then the distance between the two elements is defined as \(2^y\).

**Definition 2.6.** ([16, 17]) 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 \(2^y\).

**Definition 2.7.** ([16, 17]) 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 between the two elements is \(2^1\), 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 edges 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.

As demonstrated in [16, 17], the linear complexity of a $2^n$-periodic binary sequence with only one cube has the following nice property.

**Theorem 2.8.** 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 $2^{i_1}, 2^{i_2}, \ldots, 2^{i_m}$ $(0 \leq i_1 < i_2 < \cdots < i_m < n)$ respectively, then $L(s) = 2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m})$.

**Proof.** We give a proof based on Algorithm 2.1.

In the $k$th 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 $k$th 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 $2^{i_m}$.

\[ \cdots \]

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. \hfill \qed

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

**Algorithm 2.2**

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

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

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

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

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

**Step 4.** After above operation, we can obtain one nonzero element. Now by only restoring the nonzero elements in $Right(s^{(n)})$ removed in Step 2, so that $Left(s^{(n)}) = Right(s^{(n)})$. In this case, we obtain a cube $c_1$ with linear complexity $L(s^{(n)})$.

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

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

Obviously, this is a cube decomposition of sequence $s^{(n)}$, and we define it as the **standard cube decomposition**. One can observe that cube decomposition of a sequence may not be unique in general and the **standard cube decomposition** of a sequence described above is unique.

Next we use a sequence \{1101 1001 1000 0000\} to illustrate the decomposition process.
As \( \text{Left} \neq \text{Right} \), then we consider \( \text{Left} \oplus \text{Right} \). Then the cube \( \{1000\ 0000\ 1000\ 0000\} \) is removed.

Recursively, as \( \text{Left} \neq \text{Right} \), then we consider \( \text{Left} \oplus \text{Right} \). This time the cube \( \{0001\ 0001\ 0000\ 0000\} \) is removed. Only cube \( \{0100\ 1000\ 0000\ 0000\} \) is retained. So the standard cube decomposition is \( \{0100\ 1000\ 0000\ 0000\}, \{0001\ 0001\ 0000\ 0000\}, \{1000\ 0000\ 1000\ 0000\} \).

3. 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. in [7] showed that the first descent point of the \( k \)-error linear complexity is reached by \( k = 2H_H(2^n - L(s^{(n)})) \), where \( H_H(a) \) 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 point 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 \( i \)-th descent point of the \( k \)-error linear complexity, where \( i > 0 \). We define \( S(a) \) as the binary representation of an integer \( a \), and \( H_H(S(a)) \) denotes the Hamming weight of \( S(a) \). We further define \( L^{(i)}(s^{(n)}) \) as the \( k \)-error linear complexity of the \( i \)-th 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

\[
S^{-1}(S_1) = i_1, S^{-m}(S_1) = i_m
\]

\[
S_{>1k}(2^n - L_1) = S(2^{i_1+1} + 2^{i_2+2} + \cdots + 2^{i_m})
\]

Let \( S(a) = (x_1, x_2, \cdots, x_n) \) and \( S(b) = (y_1, y_2, \cdots, y_n) \). Then define \( S(a) \cap S(b) = (x_1y_1, x_2y_2, \cdots, x_ny_n) \), \( S(a) \cup S(b) = (x_1 + y_1 - x_1y_1, x_2 + y_2 - x_2y_2, \cdots, x_n + y_n - x_ny_n) \).

To obtain our main results, we first present the following lemma.

**Lemma 3.1.** Let \( s^{(n)} \) be a \( 2^n \)-periodic binary sequence. Assume that the second last descent 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 descent 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 descent 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 $c^{(i)}$, 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 $x + y + z$. 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 3.1, next we present a very fundamental theorem regarding CELCS, followed by an important definition called the $k$-error cube decomposition.

**Theorem 3.2.** Let $s^{(n)}$ be a $2^n$-periodic binary sequence. Then

i) $s^{(n)} = c^{(0)} + c^{(1)} + c^{(2)} + \cdots + c^{(j)}$, 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 $k^{(i+1)} = W_H(c^{(0)} + c^{(1)} + c^{(2)} + \cdots + c^{(i)}), 0 \leq i \leq j$;

ii) $s^{(n)} = c^{(0)} + c^{(1)} + c^{(2)} + \cdots + c^{(m)} + \ell^{(n)}$, where $\ell^{(i)}$ is a cube with linear complexity $L(\ell^{(i)}) = L^{(i)}(s^{(n)}), t^{(n)}_m$ is a $2^n$-periodic binary sequence with $L^{(m)}(s^{(n)}) > L(t^{(n)}_m)$, and $k^{(m+1)} \leq W_H(c^{(0)} + c^{(1)} + c^{(2)} + \cdots + c^{(m)})$.

**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 $L(c^{(j-1)}) \leq L(c^{(j)})$, as $s^{(n)} = e_j^{(n)} + c^{(j-1)} + c^{(j)}$, 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 $L(e_{j-1}^{(n)} + s^{(n)}) < L(c^{(j)})$ 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 $L(c^{(0)}) > L(c^{(1)}) > L(c^{(2)}) > \cdots > L(c^{(j)}), L^{(i)}(s^{(n)}) = L(c^{(i)}), and k^{(i)} = W_H(c^{(i)}) = W_H(c^{(0)} + c^{(1)} + c^{(2)} + \cdots + c^{(i-1)}), 0 \leq i \leq j + 1$.

ii) In the case of i), we first obtain the last cube $c^{(j)}$, then $c^{(j-1)}, c^{(j-2)}, \ldots$. 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 $s^{(n)} = e_m^{(n)} + c^{(m)} + \ell^{(n)}$, where $L(t^{(n)}_m) < L(c^{(m)})$. 


By applying the result of i) to $e^{(n)}_m$, we have that $s^{(n)} = c^{(0)} + c^{(1)} + c^{(2)} + \cdots + c^{(m)} + t^{(n)}_m$, where $L(c^{(i)}) = L(s^{(n)})$, $k^{(i)} = W_H(e^{(n)}_i) = W_H(c^{(0)} + c^{(1)} + c^{(2)} + \cdots + c^{(i-1)})$, $0 \leq i \leq m$.

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 3.2.

Example 3.1. In fact, there indeed exists the case that $k^{(m+1)} < W_H(c^{(0)} + c^{(1)} + c^{(2)} + \cdots + c^{(m)})$. Let

- $c^{(0)} = \{11001100 \ 00000000 \ 00000000 \ 00000000 \}$,
- $c^{(1)} = \{10101010 \ 10101010 \ 00000000 \ 00000000 \}$,
- $c^{(2)} = \{11001100 \ 11001100 \ 11001100 \ 11001100 \}$,
- $t^{(5)}_5 = \{11111111 \ 11111111 \ 11111111 \ 11111111 \}$,

and $s^{(5)} = c^{(0)} + c^{(1)} + c^{(2)} + t^{(5)}_5$. 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 3.2. Let

- $c^{(0)} = \{11001100 \ 00000000 \ 00000000 \ 00000000 \}$,
- $c^{(1)} = \{10101010 \ 10101010 \ 00000000 \ 00000000 \}$,
- $c^{(2)} = \{11001100 \ 11001100 \ 11001100 \ 11001100 \}$,
- $t^{(5)}_2 = \{11111111 \ 11111111 \ 11111111 \ 11111111 \}$,

and $s^{(5)} = c^{(0)} + c^{(1)} + c^{(2)} + t^{(5)}_2$. 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 3.3. We now still use the sequence $s^{(4)} = \{1101 \ 1001 \ 1000 \ 0000 \}$ to illustrate Theorem 3.2.

Let

- $c^{(0)} = \{0100 \ 1000 \ 0000 \ 0000 \}$,
- $t^{(4)}_0 = \{1001 \ 0001 \ 1000 \ 0000 \}$. Then $s^{(4)} = c^{(0)} + t^{(4)}_0$.

Let

- $c^{(0)} = \{0000 \ 1100 \ 0000 \ 0000 \}$,
- $c^{(1)} = \{0101 \ 0101 \ 0000 \ 0000 \}$,
- $t^{(4)}_1 = \{1000 \ 0000 \ 1000 \ 0000 \}$. Then $s^{(4)} = c^{(0)} + c^{(1)} + t^{(4)}_1$.

Let

- $c^{(0)} = \{0000 \ 0100 \ 0000 \ 1000 \}$,
- $c^{(1)} = \{0100 \ 0100 \ 0001 \ 0001 \}$,
- $c^{(2)} = \{1001 \ 1001 \ 1001 \ 1001 \}$,
- $t^{(4)}_2 = \{0000 \ 0000 \ 0000 \ 0000 \}$. Then $s^{(4)} = c^{(0)} + c^{(1)} + c^{(2)} + t^{(4)}_2$. 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 3.2, 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 3.2, 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 3.2 to find the second and third descent points.

**Theorem 3.3.** For a 2^n-periodic binary sequence \(s^{(n)}\), the second descent point of the k-error linear complexity is reached by

\[
k(2) = 2W_H(S(s^{(n)})) + 2W_H(S^{(1)}(s^{(n)})) - 2 \times 2W_H(S(s^{(n)}) \cap S^{(1)}(s^{(n)}))
\]

**Proof.**

i) First 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 \(k(2) = 2^0 + 2W_H(S^{(1)}(s^{(n)})) - 2 \times 2^0 = 2W_H(S^{(1)}(s^{(n)})) - 1\).

From the part two of Theorem 3.2, \(s^{(n)} = c^{(0)} + c^{(1)} + t^{(n)}\), where \(c^{(0)}\) is a 0-cube (one nonzero element), \(c^{(1)}\) is a cube with \(2W_H(S^{(1)}(s^{(n)}))\) 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 2.2, \(L^{(1)}(s^{(n)})\) 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 \(k(2) = 2W_H(S^{(1)}(s^{(n)})) - 1\).

(For example, \(u^{(4)} = \{1111 1000 0000 0000\}\). \(L^{(1)}(u^{(4)}) = 2^4 - (1 + 2)\) is achieved by a 2-cube \(\{1111 1111 0000 0000\}\). \(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 \(k(2) = 2W_H(S^{(1)}(s^{(n)})) - 1\).

ii) Second consider the case that \(L(s^{(n)}) < 2^n\).

From the part two of Theorem 3.2, suppose that \(s^{(n)} = c^{(0)} + c^{(1)} + t^{(n)}\), where \(c^{(0)}\) is a cube with \(2W_H(S(s^{(n)}))\) nonzero elements and linear complexity \(L(s^{(n)})\), and \(c^{(1)}\) is a cube with \(2W_H(S^{(1)}(s^{(n)}))\) nonzero elements and linear complexity \(L^{(1)}(s^{(n)})\), and \(L(t^{(n)}) < L^{(1)}(s^{(n)})\).

If \(W_H(c^{(0)} + c^{(1)}) = W_H(c^{(0)}) + W_H(c^{(1)})\), it is obvious that by changing \(2W_H(S(s^{(n)})) - 2W_H(S^{(1)}(s^{(n)})) + 2W_H(S^{(1)}(s^{(n)})) - 2W_H(S(s^{(n)}))\) nonzero elements, one can construct another cube \(c_2\) with linear complexity \(L^{(1)}(s^{(n)})\), and using \(2W_H(S(s^{(n)}))\) nonzero elements of \(c^{(0)}\). From Lemma 2.2, \(L(c^{(1)} + c_2) < L(c^{(1)}) = L^{(1)}(s^{(n)})\). 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 \(2W_H(S(s^{(n)})) - 2W_H(S^{(1)}(s^{(n)})) + 2W_H(S^{(1)}(s^{(n)})) - 2W_H(S(s^{(n)}))\) nonzero elements, one can still construct another cube \(c_2\) with linear complexity \(L^{(1)}(s^{(n)})\), and using \(2W_H(S(s^{(n)}))\) 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 \(k(2) = 2W_H(S(s^{(n)})) + 2W_H(S^{(1)}(s^{(n)})) - 2 \times 2W_H(S(s^{(n)})) = 2W_H(S(s^{(n)})) - 1\).
(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. \( \square \)

In fact, Chang and Wang proved this result in Theorem 3 of [1], 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 special result.

**Proposition 3.1** For a \( 2^n \)-periodic binary sequence \( s^{(n)} \), let \( k^{(i)} \) denote the \( i \)th descent point of the k-error linear complexity, \( i > 0 \). If \( S^{(i)}(s^{(n)}) \subseteq S^{(0)}(s^{(n)}) \cup S^{(1)}(s^{(n)}) \cup \cdots \cup S^{(i-1)}(s^{(n)}) \), then \( k^{(i+1)} = 2W_H(S^{(i)}(s^{(n)})) - k^{(i)}, \ i > 1 \).

**Proof.** As \( S^{(i)}(s^{(n)}) \subseteq S^{(0)}(s^{(n)}) \cup S^{(1)}(s^{(n)}) \cup \cdots \cup S^{(i-1)}(s^{(n)}) \), by changing \( 2W_H(S^{(i)}(s^{(n)})) - k^{(i)} \) elements of \( s^{(n)} \), the linear complexity of \( s^{(n)} \) becomes 0 or less than \( L^{(i)}(s^{(n)}) \). So \( k^{(i+1)} = 2W_H(S^{(i)}(s^{(n)})) - k^{(i)} \). \( \square \)

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 \( S^{(3)}(s^{(n)}) \supseteq S^{(0)}(s^{(n)}) \cup S^{(1)}(s^{(n)}) \cup S^{(2)}(s^{(n)}) \).

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 \( k^{(3)} = 3^2 - 3 = 5 \). 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 \( i \)th 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.

\[
\left| \bigcap_{i=1}^{n} A_i \right| = \sum_{i=1}^{n} |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| - \cdots + (-1)^{n-1} |A_1 \cap \cdots \cap A_n|
\]

Based on the principle of inclusion-exclusion, we give the following important theorem on the third descent point.

**Theorem 3.4.** For a \( 2^n \)-periodic binary sequence \( s^{(n)} \), let \( k^{(i)} \) denote the \( i \)th descent point of the k-error linear complexity, \( i > 0 \), and \( i_{m(S_1 \setminus S_0 S_2)} = S^{-m}(S^{(1)}(s^{(n)}) \setminus \{S^{(1)}(s^{(n)}) \cap (S^{(0)}(s^{(n)}) \cup S^{(2)}(s^{(n)))\)})\).

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) \( [i_{m(S_1 \setminus S_0 S_2)} > \min\{S^{-1}(S^{(1)}(s^{(n)}) \cap S^{(2)}(s^{(n))), S^{-1}(S^{(0)}(s^{(n)}) \cap S^{(2)}(s^{(n))))\} \)

and

\( (S^{(0)}(s^{(n)}) \cap S^{(2)}(s^{(n))) \subset S^{(1)}(s^{(n))} \} \)}
If (i) and (ii) or (i) and (iii) hold, then
\begin{align*}
k(3) &= 2W_H(S(0)(s(n))) + 2W_H(S(1)(s(n))) + 2W_H(S(2)(s(n))) \\
&\quad - 2 \times 2W_H(S(0)(s(n)) \cap S(1)(s(n))) - 2 \times 2W_H(S(0)(s(n)) \cap S(2)(s(n))) \\
&\quad - 2 \times 2W_H(S(1)(s(n)) \cap S(2)(s(n))) + 2 \times 2W_H(S(0)(s(n)) \cap S(1)(s(n)) \cap S(2)(s(n))).
\end{align*}

Otherwise, we have
\begin{align*}
k(3) &= 2W_H(S(0)(s(n))) + 2W_H(S(1)(s(n))) + 2W_H(S(2)(s(n))) \\
&\quad - 2 \times 2W_H(S(0)(s(n)) \cap S(1)(s(n))) - 2 \times 2W_H(S(0)(s(n)) \cap S(2)(s(n))) \\
&\quad - 2 \times 2W_H(S(1)(s(n)) \cap S(2)(s(n))) + 4 \times 2W_H(S(0)(s(n)) \cap S(1)(s(n)) \cap S(2)(s(n))).
\end{align*}

Proof. The following proof is based on the framework that \( s(n) = c(0) + c(1) + c(2) + \cdots + c(i) + t(n) \). 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 \( c(0) \), so that \( L(c(i)) = L(c(1)) \) and the linear complexity of \( c(0) + c(1) + c(2) + \cdots + c(i) \) becomes 0 by changing \( k(i+1) \) elements, which implies that \( c(0) + c(1) + c(2) + \cdots + c(i) \) has exactly \( k(i+1) \) nonzero elements.

Therefore the computation of \( k(i+1) \) is equivalent to counting the nonzero elements of \( c(0) + c(1) + c(2) + \cdots + c(i) \).

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 \( W_H(c(0)) + W_H(c(1)) - 2 \times 2W_H(S(c(0)) \cap S(c(1))) \).

From Theorem 3.2, 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 3.3, \( k(2) = 2W_H(c(0)) + 2W_H(c(1)) - 2 \times 2W_H(S(c(0)) \cap S(c(1))) \). After changing \( k(2) \) nonzero elements, the sequence becomes \( c(2) + t(n) \), where \( L(t(n)) < L(2)(s(n)) \).

Thus \( W_H(c(0) + c(1)) = 2W_H(c(0)) + 2W_H(c(1)) - 2 \times 2W_H(S(c(0)) \cap S(c(1))) \).

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 \( k(2) = 2W_H(c(0)) + 2W_H(c(1)) - 2 \times 2W_H(S(c(0)) \cap S(c(1))) \) nonzero elements.

We construct a cube \( c(2) \) with linear complexity \( L(2)(s(n)) \), and furthermore, we consider the superposition of \( c(0) \), \( c(1) \) and \( c(2) \) with the alignment of first nonzero elements of three cubes. Then with an analysis similar to the principle of inclusion-exclusion, we have that \( c(0) + c(1) + c(2) \) has exactly \( 2W_H(S(c(0))) + 2W_H(S(c(1))) + 2W_H(S(c(2))) - 2 \times 2W_H(S(c(0)) \cap S(c(1))) - 2 \times 2W_H(S(c(0)) \cap S(c(2))) - 2 \times 2W_H(S(c(1)) \cap S(c(2))) + 4 \times 2W_H(S(c(0)) \cap S(c(1)) \cap S(c(2))) \) nonzero elements.

By adding \( c(0) + c(1) + c(2) \) to \( s(n) = c(0) + c(1) + c(2) + t(n) \), we have \( c(1) + c(2) + t(n) \). From Lemma 2.2, \( L(c(1) + c(2)) < L(2)(s(n)) \). Thus \( k(3) \leq W_H(c(0) + c(1) + c(2)) = 2W_H(S(c(0)) + 2W_H(S(c(1))) + 2W_H(S(c(2))) - 2 \times 2W_H(S(c(0)) \cap S(c(1))) - 2 \times 2W_H(S(c(0)) \cap S(c(2))) - 2 \times 2W_H(S(c(1)) \cap S(c(2))) + 4 \times 2W_H(S(c(0)) \cap S(c(1)) \cap S(c(2))) \).

(For example, let \( c(0) = \{11000000 11000000 00000000 00000000 00000000 00000000 00000000 00000000\}, \)
$c^{(1)} = \{10101010 \ 00000000 \ 01010101 \ 00000000 \ 00000000 \ 00000000 \ 00000000 \ 00000000 \}.$
$c^{(2)} = \{11110000 \ 00000000 \ 00000000 \ 00000000 \ 00000000 \ 00000000 \ 00000000 \ 00000000 \}.$

Then $c^{(0)} + c^{(1)} + c^{(2)}$ has exactly $2^{W_H(S(c^{(0)}))} + 2^{W_H(S(c^{(1)}))} + 2^{W_H(S(c^{(2)}))} - 2 \times 2^{W_H(S(c^{(0)}) \cap S(c^{(1)}))} - 2 \times 2^{W_H(S(c^{(0)}) \cap S(c^{(2)}))} - 2 \times 2^{W_H(S(c^{(1)}) \cap S(c^{(2)}))} + 4 \times 2^{W_H(S(c^{(0)}) \cap S(c^{(1)}) \cap S(c^{(2)}))} = 4 + 8 + 8 - 2 - 4 + 4 = 14$ 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 $[i_{m(S^{1}\cup S^{2})} > \min \{S^{(0)}(s^{(n)}) \cap S^{(2)}(s^{(n)}), S^{(1)}(s^{(n)}) \cap S^{(1)}(s^{(n)})\}]$ and $(S^{(0)}(s^{(n)}) \cap S^{(2)}(s^{(n)}) \cap (S^{(0)}(s^{(n)}) \cap S^{(2)}(s^{(n)}))]$, we try to construct a cube $c_2^{(2)}$ with linear complexity $L(c^{(2)})$, so that $c^{(0)} + c^{(1)} + c^{(2)}$ 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 $[i_{m(S^{1}\cup S^{2})} > S^{(0)}(s^{(n)}) \cap S^{(2)}(s^{(n)}) \cap S^{(1)}(s^{(n)}) \cap S^{(2)}(s^{(n)})\}$ and $(S^{(0)}(s^{(n)}) \cap S^{(2)}(s^{(n)}) \cap S^{(0)}(s^{(n)}) \cap S^{(2)}(s^{(n)}))]$, 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 $c^{(0)} + c^{(1)} + c^{(2)}$, where $c^{(2)}$ is the new cube with linear complexity $L(c^{(2)})$.

We follow the above example, let,

$c_2^{(2)} = \{01111000 \ 00000000 \ 00000000 \ 01111000 \ 00000000 \ 00000000 \}.$

Then $c^{(0)} + c^{(1)} + c^{(2)}$ has $4 + 8 + 8 - 2 - 4 + 4 = 12$ 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

$c^{(0)} = \{10100000 \ 10100000 \ 00000000 \ 00000000 \ 00000000 \ 00000000 \ 00000000 \ 00000000 \}.$
$c^{(1)} = \{11001100 \ 00000000 \ 11001100 \ 00000000 \ 00000000 \ 00000000 \ 00000000 \ 00000000 \}.$
$c^{(2)} = \{10101010 \ 00000000 \ 10101010 \ 00000000 \ 01010101 \ 00000000 \ 01010101 \ 00000000 \}.$

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 $S(c^{(0)}) \cap S(c^{(2)}) = \{000010\}, S(c^{(1)}) \cap S(c^{(2)}) = \{010100\}, S(c^{(1)}) \cap S(c^{(2)}) = \{00001\}, S(c^{(2)}) = \{000000\}, 1 < S^{-m}\{00001\} = 2 < S^{-1}\{010100\} = 4.$

Assume that $c^{(2)} = \{01010101 \ 00000000 \ 01010101 \ 00000000 \ 01010101 \ 00000000 \}.$

Then $c^{(0)} + c^{(1)} + c^{(2)}$ 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 3.4.

**Example 3.4.** Let $c^{(0)} = \{10001000 \ 00000000 \ 00000000 \ 00000000 \ 00000000 \ 00000000 \ 00000000 \ 00000000 \}.$
Let $\{11000000 11000000 11000000 00000000 00000000 00000000 00000000\}$, 
$\{11111111 00000000 11111111 00000000 11111111 00000000 11111111 00000000\}$.

Then $S(c^{(0)}) = \{001000\}, S(c^{(1)}) = \{011001\}, S(c^{(2)}) = \{110111\}$. $W_H([S(c^{(0)}) \cap S(c^{(1)})] \cup (S(c^{(1)}) \cap S(c^{(2)}))] = 2 < W_H(S(c^{(1)})) = 3$ and $S(c^{(0)}) \cap S(c^{(2)}) = \{001000\} \supset S(c^{(1)}) \cap S(c^{(2)}) = \{000000\}$.

As $S(c^{(1)}) \cap S(c^{(2)}) = \{010001\}$, $S(c^{(1)}) \cap (S(c^{(0)}) \cup S(c^{(2)}))] = \{110000\}$, $i_{m(S(1) \cup S(2))}(c^{(0)}) \cap S_{m(S(1) \cup S(2))}(c^{(2)}) = \{000000\}$, thus this is the case that $i_{m(S(1) \cup S(2))} = \min\{S^{-1}(S^{(1)}(s(n)) \cap S^{(2)}(s(n))), S^{-1}(S^{(0)}(s(n)) \cap S^{(2)}(s(n)))\}$ and $(S^{(0)}(s(n)) \cap S^{(2)}(s(n))) \subset S^{(1)}(s(n)))].$

We move the first $2W_H(S(c^{(0)}) \cap S(c^{(1)}) \cap S(c^{(2)}))]$ nonzero elements in $c^{(2)}$ to the location below the not cancelled nonzero elements in $c^{(1)}$. Let, 
$c^{(2)} = \{01111111 10000000 01111111 10000000 01111111 10000000 \}.$

It is obvious that $c^{(0)} + c^{(1)} + c^{(2)}$ contains exactly $2^2 + 2^3 + 2^4 - 2 \times 2^0 - 2 \times 2^1 - 2 \times 2^2 + 2 \times 2^0 = 30$ nonzero elements. So $k^{(3)} = 30$.

**Example 3.5.** Let
$c^{(0)} = \{11001100 00000000 00000000 00000000\},$
$c^{(1)} = \{10101010 10101010 00000000 00000000\},$
$c^{(2)} = \{11001100 11001100 11001100 11001100\}.$

Then $S(c^{(0)}) = \{00101\}, S(c^{(1)}) = \{01110\}, S(c^{(2)}) = \{11011\}$. $W_H([S(c^{(0)}) \cap S(c^{(1)})] \cup (S(c^{(1)}) \cap S(c^{(2)}))] = 2 < W_H(S(c^{(1)})) = 3$ and $S(c^{(0)}) \cap S(c^{(2)}) = \{00101\} \supset S(c^{(1)}) \cap S(c^{(2)}) = \{00000\}$.

As $S(c^{(1)}) \cap S(c^{(2)}) = \{01100\}$, $S(c^{(1)}) \cap (S(c^{(0)}) \cup S(c^{(2)}))] = \{00110\}$, 
$i_{m(S(1) \cup S(2))}(c^{(0)}) \cap S_{m(S(1) \cup S(2))}(c^{(2)}) = \{00000\}$, $S_{m(S(1) \cup S(2))}(c^{(2)}) = \{00100\} = \min\{S^{-1}(S^{(1)}(s(n)) \cap S^{(2)}(s(n))), S^{-1}(S^{(0)}(s(n)) \cap S^{(2)}(s(n)))\}$ and $(S^{(0)}(s(n)) \cap S^{(2)}(s(n))) \subset S^{(1)}(s(n)))].$

We move the first $2W_H(S(c^{(0)}) \cap S(c^{(1)}) \cap S(c^{(2)}))]$ nonzero elements in $c^{(2)}$ to the location below the not cancelled nonzero elements in $c^{(1)}$. Let, 
$c^{(2)} = \{01100110 01100110 01100110 \}.$

It is obvious that $c^{(0)} + c^{(1)} + c^{(2)}$ contains exactly $2^2 + 2^3 + 2^4 - 2 \times 2^1 - 2 \times 2^2 + 2 \times 2^0 = 12$ nonzero elements. So $k^{(3)} = 12$.

**Example 3.6.** Let
$c^{(0)} = \{11110000 00000000 00000000 00000000 00000000 \},$
$c^{(1)} = \{11111111 00000000 00000000 00000000 00000000 \},$
$c^{(2)} = \{11111111 00000000 11111111 00000000 11111111 00000000 \}.$

Then $S(c^{(0)}) = \{000011\}, S(c^{(1)}) = \{011111\}, S(c^{(2)}) = \{110111\}$. $W_H([S(c^{(0)}) \cap S(c^{(1)})] \cup (S(c^{(1)}) \cap S(c^{(2)}))] = 3 < W_H(S(c^{(1)})) = 4$ and $S(c^{(0)}) \cap S(c^{(2)}) = S(c^{(0)}) \cap S(c^{(1)}) \cap S(c^{(2)}) = \{00001\}$.

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 $2W_H(S(c^{(0)}) \cap S(c^{(1)}) \cap S(c^{(2)}))]$ nonzero elements in $c^{(2)}$ to the location below the not cancelled nonzero elements in $c^{(1)}$. Let, 
$c^{(2)} = \{00001111 11110000 00001111 11110000 00001111 11110000 \}.$
It is obvious that $c^{(0)} + c^{(1)} + c^{(2)} - 1$ contains exactly $2^2 + 2^4 + 2^5 - 2 \times 2^2 - 2 \times 2^2 - 2 \times 2^3 + 2 \times 2^2 - 2 \times 2^5 + 2 \times 2^2 = 28$ nonzero elements. So $k^{(3)} = 28$.

For $k^{(3)}$, it is easy to verify that Proposition 3.1 is the special case of Theorem 3.4.

We have tested all $2^n$-periodic binary sequences ($n = 4, 5$) by a computer program to verify Theorem 3.4.

4. Conclusions. In this paper, we first propose the $k$-error cube decomposition for $2^n$-periodic binary sequences. By applying the famous inclusion-exclusion principle, we obtain the complete characterization of the $i$th descent point (critical point) of the $k$-error linear complexity for $i = 2, 3$.

In previous research, investigators mainly focus on the linear complexity and $k$-error complexity for a given sequence. In contrast, the proposed constructive approach can be used to construct $2^n$-periodic binary sequences with the given linear complexity and $k$-error linear complexity (or CELCS). This is a challenging problem with broad applications. We will continue this work in future due to its importance. Based on the results obtained here, another interesting future direction is to investigate the expected drop of the linear complexity after the $i$th descent point for $i = 1, 2, 3$.

REFERENCES

[1] Z. L. Chang and X. Y. Wang, On the First and Second Critical Error Linear Complexity of Binary $2^n$-periodic Sequences, *Chinese Journal of Electronics*, **22** (2013), 1–6.

[2] C. S. Ding, G. Z. Xiao and W. J. Shan, *The Stability Theory of Stream Ciphers[M]*, Lecture Notes in Computer Science, Vol.561. Berlin/ Heidelberg, Germany: Springer-Verlag, 1991.

[3] T. Etzion, N. Kalouptsidis, N. Kolokotronis, K. Limniotis and K. G. Paterson, Properties of the error linear complexity spectrum, *IEEE Transactions on Information Theory*, **55** (2009), 4681–4686.

[4] F. Fu, H. Niederreiter and M. Su, The characterization of $2^n$-periodic binary sequences with fixed 1-error linear complexity, In: Gong G., Helleseth T., Song H.-Y., Yang K. (eds.) *SETA 2006*, LNCS, **4086** (2006), 88–103. Springer.

[5] R. A. Games and A. H. Chan, A fast algorithm for determining the complexity of a binary sequence with period $2^n$, *IEEE Trans on Information Theory*, **29** (1983), 144–146.

[6] N. Kolokotronis, P. Rizomiliotis and N. Kalouptsidis, Minimum linear span approximation of binary sequences, *IEEE Transactions on Information Theory*, **48** (2002), 2758–2764.

[7] K. Kurosawa, F. Sato, T. Sakata and W. Kishimoto, A relationship between linear complexity and $k$-error linear complexity, *IEEE Transactions on Information Theory*, **46** (2000), 694–698.

[8] A. Lauder and K. Paterson, Computing the error linear complexity spectrum of a binary sequence of period $2^n$, *IEEE Transactions on Information Theory*, **49** (2003), 273–280.

[9] J. L. Massey, Shift register synthesis and BCH decoding, *IEEE Trans on Information Theory*, **15** (1969), 122–127.

[10] W. Meidl, How many bits have to be changed to decrease the linear complexity?, *Des. Codes Cryptogr.*, **33** (2004), 109–122.

[11] W. Meidl, On the stability of $2^n$-periodic binary sequences, *IEEE Transactions on Information Theory*, **51** (2005), 1151–1155.

[12] R. A. Rueppel, *Analysis and Design of Stream Ciphers*, Berlin: Springer-Verlag, 1986, chapter 4.

[13] M. Stamp and C. F. Martin, An algorithm for the $k$-error linear complexity of binary sequences with period $2^n$, *IEEE Trans. Inform. Theory*, **39** (1993), 1398–1401.

[14] J. Q. Zhou, On the $k$-error linear complexity of sequences with period $2^p$ over GF(q), *Des. Codes Cryptogr.*, **58** (2011), 279–296.

[15] J. Q. Zhou and W. Q. Liu, The $k$-error linear complexity distribution for $2^n$-periodic binary sequences, *Des. Codes Cryptogr.*, **73** (2014), 55–75.
[16] J. Q. Zhou, W. Q. Liu and G. L. Zhou, Cube theory and stable $k$-error linear complexity for periodic sequences, Inscrypt, LNCS, 8567 (2013), 70–85.

[17] J. Q. Zhou and W. Q. Liu, On the $k$-error linear complexity for $2^n$-periodic binary sequences via Cube Theory, 2013, http://arxiv.org/abs/1309.1829.

[18] F. X. Zhu and W. F. Qi, The 2-error linear complexity of $2^n$-periodic binary sequences with linear complexity $2^n-1$, Journal of Electronics (China), 24 (2007), 390–395.

Received December 2014; 1st revision August 2016; 2nd revision August 2016.

E-mail address: zhou9@yahoo.com
E-mail address: w.liu@curtin.edu.au
E-mail address: wxf80106@163.com