On the Second Descent Points for the K-Error Linear Complexity of 2^n-Periodic Binary Sequences

Jianqin Zhou[1,2,*], Xifeng Wang[1] and Wanquan Liu[2]
[1]School of Computer Science, Anhui Univ. of Technology, Ma'anshan, 243032 China
[2]Department of Computing, Curtin University, Perth, WA 6102 Australia
[*]Corresponding author

***Abstract*—In this paper, a constructive approach for determining CELCS (critical error linear complexity spectrum) for the k-error linear complexity distribution of 2^n-periodic binary sequences is developed via the sieve method and Games-Chan algorithm. Accordingly, the second descent point (critical point) distribution of the k-error linear complexity for 2^n-periodic binary sequences is characterized. As a by product, 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}<=k < 2^l and l < n. With these results, some work by Niu et al. are proved to be incorrect.**

Keywords-periodic sequence; linear complexity; k-error linear complexity; k-error linear complexity distribution

I. INTRODUCTION

The CELCS (critical error linear complexity spectrum) is studied in [11], [3]. In fact they are the points where a decrease occurs for the k-error linear complexity, and thus are called critical points. The third descent point distribution of the 5-error linear complexity for 2^n-periodic binary sequences are characterized completely in [24].

In this paper, we present a constructive approach for determining CELCS for 2^n-periodic binary sequences based on the idea reported in [22], [24]. Accordingly, the second descent point (critical point) distribution of the k-error linear complexity for 2^n-periodic binary sequences is characterized. As a consequence, we obtain the complete counting functions on the k-error linear complexity as the second descent point of 2^n-periodic binary sequences for k = 3; 4. We expect that with the constructive approach proposed here, one can further obtain other second and third descent point distribution of the k-error linear complexity for 2^n-periodic binary sequences.

In [22], we investigate all 2^n-periodic binary sequences with the given 3-error linear complexity. In contrast, here we only investigate the 2^n-periodic binary sequence with the given 3-error linear complexity, where the second decrease occurs exactly at 3-error linear complexity. So the study here is more accurate. As a by product, it is proved that the maximum k-error linear complexity is 2^n- (2^l -1) over all 2^n-periodic binary sequences. With these results, some work by Niu et al. [15], [16] are proved to be incorrect.

II. PRELIMINARIES

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

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

If $q = 2$, we denote $x + y$ as $x \oplus y$ as well. When $n = 2m$, we define $Left(x) = (x_1, x_2, \cdots, x_m)$ and $Right(x) = (x_{m+1}, x_{m+2}, \cdots, x_{2m})$.

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

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

Algorithm 2.1

Input:

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

Output: $L(s) = c$.

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

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

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

The following lemmas are well known results on 2^n-periodic binary sequences and are required in this paper. Please refer to [14], [8], [22], [25] for details.

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

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

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

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

III. Counting Functions for 2^N-Periodic Binary Sequences with Given 3-Error Linear Complexity

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 k_1-error linear complexity and second descent point k_2-error linear complexity.

Theorem 3.1 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: ==>

By result from Kurosawa et al. [10] 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 $L_1(s^{(n)}) = 2^n - (2^i + 2^j)$.

<==

Suppose that $L_1(s^{(n)}) =2^n - (2^i + 2^j)$. Similarly by result from Kurosawa et al. [10] we know that it is possible to change 3 elements of $s^{(n)}$, so that the new sequence with linear complexity less then $2^n - (2^i + 2^j)$. That is $L_3(s^{(n)}) < L_1(s^{(n)})$. ■

Next we investigate the distribution of $L_3(s^{(n)})$.

Theorem 3.2 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 $L_3(s^{(n)}) = 2^n - (2^{i1} + 2^{i2} + \ldots + 2^{im}) < 2^n -(2^i + 2^j)$, where $0\leq i_1 < i_2 < \ldots < i_m < n$, $m > 2$, or $L_3(s^{(n)}) = 2^n - (2^{i1} + 2^{i2}) < 2^n -(2^i + 2^j)$, 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 a 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 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 3.3 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 $L_3(s^{(n)}) = 2^n - (2^{i1}+2^{i2}+\ldots +2^{im}) < 2^n -(2^i+2^j)$, where $0 \leq i_1 < i_2 < \ldots < i_m < n$, $m > 2$ or $L_3(s^{(n)}) = 2^n -(2^{i1} +2^{i2}) < 2^n -(2^i+2^j)$, 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

$$2^{3n-j-i-3} \times 2^{L-1}/(2^{\varepsilon+j-i0} \times 8^{n-im-1})$$

where $i_0 \leq j$ is the minimum number for which $2^n - (2^{i0} + 2^j) < 2^n - (2^{i1} + 2^{i2} + \ldots + 2^{im})$ with a default choice $i_0 = j$. Further, if $j = i_m$ or $2^n - (2^j + 2^{im}) > L_3(s^{(n)})$ then $\varepsilon = 0$; if $j < i_m$ and only $2^n - (2^j + 2^{im}) < L_3(s^{(n)})$ then $\varepsilon = 1$; if $2^n - (2^i + 2^{im}) < L_3(s^{(n)})$ then $\varepsilon = 2$, where $i_m = i_2$ for $L = 2^n - (2^{i1} + 2^{i2})$.

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: Due to the page limit, the detailed proof is omitted.

IV. Counting Functions for 2^N-Periodic Binary Sequences with Given 4-Error Linear Complexity

Next we will use Cube Theory, which is introduced in [23]. Cube theory and some related results are presented next for completeness.

First we review some definitions.

Definition 4.1 Suppose that the difference of positions of two non-zero elements of sequence s is $(2x + 1)2^y$, both x and y are non-negative integers. Then the distance between the two elements is defined as 2^y.

Definition 4.2 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 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 4.3 A non-zero element of sequence s is called a vertex. Two vertexes can form an edge. If the distance between the two elements (vertices) is 2^y, then the length of the edge is defined as 2^y.

In [23], we have considered the linear complexity of a sequence with only one cube.

Theorem 4.1 Suppose that s is a binary sequence with period 2^n, and non-zero elements of s form an m-cube, if lengths of edges are $2^{i_1}, 2^{i_2}, \cdots, 2^{i_m}$ $(0 \le i_1 < i_2 < \cdots < i_m < n)$ respectively, then $L(s) = 2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m})$.

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

Algorithm 4.1

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

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

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

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

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

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

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

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

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

By Theorem 4.1, we can obtain the following results on k-error linear complexity.

Corollary 4.1 Suppose that s is a binary sequence with period 2^n and its Hamming weight is even, then the maximum $2^{k-1}, \ldots, (2^k-2)$ or (2^k-1)-error linear complexity of sequence s are all $2^n-(2^k-1)(k > 0)$.

Niu et al. in [15], [16] gave the following result.

Conjecture 4.1 Let $L_m(s)$ the m-error linear complexity of binary sequence with period 2^n. Then $L_m(s) \le 2^n - 2^m + 1$.

Corollary 4.1 completely answers Conjecture 4.1. 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 4.1 is correct only when $m = 2^{l-1}$, in other cases it is not correct.

It is known by result from Kurosawa et al. [10] that for a 2^n-periodic binary sequence with linear complexity $2^n - (2^i + 2^j)$, $0 \le i < j < n$, 4-error linear complexity is the first descent point. However, with cube theory we will characterize 2^n-periodic binary sequences with 4-error linear complexity as the second descent point.

Theorem 4.2 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 $L_2(s^{(n)}) = 2^n - (2^i + 2^j)$, $0 \le i < j < n$, but $L_2(s^{(n)}) \neq 2^n - (1 + 2)$;

iii). If $L(s^{(n)}) = 2^n - 2^{i0}$, then $i_0 < i$ or $i < i_0 < j$.

Proof: Due to the page limit, the detailed proof is omitted.

Next we investigate the distribution of $L_4(s^{(n)})$.

Theorem 4.3 Let $s^{(n)}$ be a 2^n-periodic binary sequence with linear complexity $L(s^{(n)}) = 2^n - 2^{i0}$. If $L_4(s^{(n)}) < L_2(s^{(n)}) < L(s^{(n)})$ and $L_2(s^{(n)}) = 2^n - (2^i + 2^j)$, $0 \le i < j < n$, then $L_4(s^{(n)}) = 2^n - (2^{i1} + 2^{i2} + \ldots + 2^{im}) < 2^n - (2^i + 2^j)$, where $0 \le i_1 < i^2 < \ldots < i_m < n$, $m > 3$, or $L_4(s^{(n)}) = 2^n - (2^{i1} + 2^{i2} + 2^{i3})$, where $\{i_1, i_2, i_3\} \neq \{i, j, i_0\}$, $\{i_1, i_2, i_3\} \neq \{0, 1, 2\}$, or $L_4(s^{(n)}) = 2^n - (2^{i1} + 2^{i2}) < 2^n - (2^i + 2^j)$, where $i_2 \neq j$, $i_1 \neq i, j, i_0$.

Proof: Due to the page limit, the detailed proof is omitted.

V. CONCLUSIONS

By studying the linear complexity of binary sequences with period 2^n, especially the decrease issue of linear complexity associated with the superposition of two sequences having the same linear complexity, a new approach to determining CELCS for the k-error linear complexity distribution of 2^n-periodic binary sequences was developed via the sieve method and Games-Chan algorithm. The second descent point distribution of the k-error linear complexity for 2^n-periodic binary sequences was characterized completely for $k = 3; 4$.

We expect that with the techniques proposed in this paper, one can obtain other second and third descent point distribution 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.

REFERENCES

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

[2] Ding, C. S., Xiao, G. Z. and Shan, W. J., The Stability Theory of Stream Ciphers[M]. Lecture Notes in Computer Science, Vol.561. Berlin/ Heidelberg, Germany: Springer-Verlag, 1991,85-88.

[3] Etzion T., Kalouptsidis N., Kolokotronis N., Limniotis K. and Paterson K. G., Properties of the Error Linear Complexity Spectrum, IEEE Transactions on Information Theory, 2009, 55(10): 4681-4686.

[4] Games, R. A., and Chan, A. H., A fast algorithm for determining the complexity of a binary sequence with period 2^n. IEEE Trans on Information Theory, 1983, 29(1):144-146.

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

[6] Han Y. K., Chung J. H., and Yang K., On the k-error linear complexity of pm-periodic binary sequences. IEEE Transactions on Information Theory, 2007, 53(6): 2297-2304.

[7] Kaida T., Uehara S., and Imamura K., An algorithm for the k-error linear complexity of sequences over $GF(p^m)$ with period p^n, p a prime. Information and Computation, 1999,151(1):134 -147.

[8] Kavuluru R., Characterization of 2n-periodic binary sequences with fixed 2-error or 3-error linear complexity, Des. Codes Cryptogr. 2009,53: 75-97.

[9] Kolokotronis N., Rizomiliotis P. and Kalouptsidis N., Minimum linear span approximation of binary sequences. IEEE Transactions on Information Theory, 2002, 48:2758-2764.

[10] Kurosawa K., Sato F., Sakata T. and Kishimoto W., A relationship between linear complexity and k-error linear complexity. IEEE Transactions on Information Theory, 2000, 46(2): 694-698.

[11] Lauder A. and Paterson K., Computing the error linear complexity spectrum of a binary sequence of period 2n. IEEE Transactions on Information Theory, 2003, 49(1):273-280.

[12] Massey, J. L., Shift register synthesis and BCH decoding. IEEE Trans on Information Theory, 1969, 15(1): 122-127.

[13] Meidl W., How many bits have to be changed to decrease the linear complexity?, Des. Codes Cryptogr., 2004, 33:109-122.

[14] Meidl W., On the stablity of 2^n-periodic binary sequences. IEEE Transactions on Information Theory, 2005, 51(3): 1151-1155.

[15] Niu, Z., Li, Z., Li, Z., and Xin, M., The research and analysis of the excellent 2n periodic binary sequence based on cat swarm optimization. Journal of Electronics and Information Technology (China), 2013, 35(6), 1365-1370.

[16] Niu, Z., Ye, F., Xin, M., and Wang, C., Generation and analysis of the excellent 2n-periodic binary sequences. Journal of Xidian University (China), 2014, 41(1), 130-134.

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

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

[19] Wei, S. M., Xiao, G. Z., and Chen, Z., A fast algorithm for determining the minimal polynomial of a sequence with period $2p^n$ over GF(q), IEEE Trans on Information Theory, 2002, 48(10):2754-2758.

[20] Xiao, G. Z., Wei, S. M., Lam K. Y., and Imamura K., A fast algorithm for determining the linear complexity of a sequence with period p^n over GF(q). IEEE Trans on Information Theory, 2000, 46:2203-2206.

[21] Zhou, J. Q., On the k-error linear complexity of sequences with period $2p^n$ over GF(q), Des. Codes Cryptogr., 2011, 58(3):279-296.

[22] Zhou, J. Q., Liu, W. Q., The k-error linear complexity distribution for 2^n-periodic binary sequences, Des. Codes Cryptogr., 2014, 73(1):55-75.

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

[24] Zhou, J. Q., Liu, W. Q., and Wang, X. F., 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, vol. 9543, 169-183. Springer (2015).

[25] Zhu, F. X. and Qi, W. F., The 2-error linear complexity of 2^n-periodic binary sequences with linear complexity 2^n-1. Journal of Electronics (China), 2007,24(3): 390-395, http://www.springerlink.com/content /3200vt810p232769/J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.