Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 154 (2019) 389–399

Procedia Computer Science

www.elsevier.com/locate/procedia

8th International Congress of Information and Communication Technology, ICICT 2019

The 4-Variance Linear Complexity Distribution with 2^n-Periodical Binary Sequences

Xiao Lin Wang[a],*, Jian Qin Zhou[a]

[a]*School of Computer Science and Technology, Anhui University of Technology, Ma'anshan, 243032, China*

Abstract

In this paper, the method of calculating the k-variance linear complexity distribution with 2^n-periodical sequences by the Games-Chan algorithm and sieve approach is affirmed for its generality. The main idea of this method is to decompose a binary sequence into some subsequences of critical requirements, hence the issue to find k-variance linear complexity distribution with 2^n-periodical sequences becomes a combinatorial problem of these binary subsequences. As a result, we compute the whole calculating formulas on the k-variance linear complexity with 2^n-periodical sequences of linear complexity less than 2^n for k = 4, 5. With combination of results in the whole calculating formulas on the 3-variance linear complexity with 2^n-periodical binary sequences of linear complexity 2^n, we completely solve the problem of the calculating function distributions of 4-variance linear complexity with 2^n-periodical sequences elegantly, which significantly improves the results in the relating references.

Keywords: Periodical binary sequence; linear complexity; k-variance linear complexity distribution

1. Introduction

The definition of linear complicacy is of great importance in the security research of stream ciphers and it has been the hot topic in cryptographic community [2], [14]. It is defined that the linear complicacy $L(s)$ of series s

* Corresponding author. Tel.: +86-189-0555-3721.
E-mail address: wxl@ahut.edu.cn

1877-0509 © 2019 The Authors. Published by Elsevier Ltd.

10.1016/j.procs.2019.06.056

is the length of the smallest linear feedback shift register (LFSR) that can produce series s. The weight complicacy, as a measure on the linear complicacy of periodical series, was first presented in 1990 [1]. An advanced complicated method, where called as sphere complicacy, was presented by Ding, Xiao and Shan in 1991 [2]. Stamp and Martin [14] defined the k-variance linear complicacy, which is almost the same as the sphere complicacy. Precisely, suppose that s is a periodic series of period N. For any $k(0 \leq k \leq N)$, the k-variance linear complicacy $L_k(s)$ of periodic series s is calculated as the shortest linear complicacy that can be reached when any k or fewer elements of the periodic series are altered in one period.

Rueppel [13] obtained the account of 2^n-periodical series with fixed linear complicacy L, $0 \leq L \leq 2^n$. When $k = 1$ and $k = 2$, Meidl [12] derived the whole calculating formulas on the k-variance linear complicacy with 2^n-periodical series with linear complicacy 2^n. When $k = 2$ and $k = 3$, Zhu and Qi [17] further characterized the whole calculating formulas on the k-variance linear complicacy with 2^n- periodical series with linear complicacy $2^n - 1$. With combinatorial and algebraic methods, Fu et al. [5] gaved the 2^n-periodical series with the 1-variance linear complicacy and obtained the calculating function completely for the 1-variance linear complicacy of 2^n-periodical series.

By studying periodical series with linear complicacy 2^n and linear complicacy less than 2^n together, Kavuluru [8] derived 2^n-periodical series with the 2-variance and 3-variance linear complicacy, and characterized the calculating formulas for the account of 2^n-periodical series with the k-variance linear complicacy for $k = 2$ and $k = 3$. In [16], it is proved that the calculating formulas in [8] for the account of 2^n-periodical series with the 3-variance linear complicacy are inaccurate in some cases. Further, the whole calculating formulas for the account of 2^n-periodical series with the 3-variance linear complicacy are derived in [16].

The main idea here is that we adopt a structural method for studying the k-variance linear complicacy distribution with 2^n-periodical series reported in [16], where the sieve method and Games-Chan algorithm are mainly used. The proposed approach is different from those in [5], [12], [17], and it is derived from the next main framework. Let S be $\{s|L(s) = c\}$, E be $\{e|W_H(e) = k\}$ and SE be $\{s + e|s \in S, e \in E\}$, where s and e are two periodical series. In [16], the case of $k = 3$ is studied and we will investigate the cases for $k = 4, 5$. For this purpose, we need to investigate two cases. One is to exclude all periodical series $s + u \in SE$, with $L_k(s + u) < c$. Based on Lemma 2.2 in the next section, this is equal to checking whether there exists a periodic series v so that $L(v + u) = c$. The other case is to check the repetition of some periodical series in SE with the condition that $s + u, t + v \in SE$ and $L_k(s + u) = L_k(t + v) = c$ with $s \neq t$, $u \neq v$, however $s + u = t + v$. Similarly, this is equal to checking whether there exists a periodic series v with the condition that $L(v + u) = L(s + t) < c$ and if so, check the account of such periodical series. In summary, we want to sieve periodical series $s + e$ with $L_k(s + e) = c$ from SE.

With above analysis, the issue to find k-variance linear complicacy distribution with 2^n-periodical series becomes a combinatorial problem of these periodical subsequences. With developed calculating techniques, the 4-variance linear complicacy distribution with 2^n-periodical series is solved completely. In this process, the most difficult part of the problem for the k-variance linear complicacy distribution is to compute all the possible combinations of these periodical subsequences, which becomes extremely complicated for large k. With combination of results in the whole calculating formulas on the 3-variance linear complicacy with 2^n-periodical series with *linear complicacy* 2^n, we completely solve the problem of the calculating function distributions of 4-variance linear complicacy with 2^n-periodical series elegantly, which very significantly improves the results in [8], [16].

We organize the rest of this work as follows. An outline about our main method is first given in Section 2 to compute the k-variance linear complicacy distribution with 2^n-periodical sequences for $k = 4, 5, 6$ and 7. In Section 3, we fully characterize the calculating formulas on the k-variance linear complicacy with 2^n-periodical series with *linear complicacy less than* 2^n for $k = 4, 5$. In Section 4, the conclusions are given.

2. The main idea of the proposed structural method

In this part, some preliminary results are first given. We also present an outline about the proposed method to determine the k-variance linear complicacy distribution with 2^n-periodical series for $k = 4, 5, 6$ and 7.

Suppose that $y = (y_1, y_2, \cdots, y_n)$ and $x = (x_1, x_2, \cdots, x_n)$ are vectors over $GF(q)$. Then define $y + x = (y_1 + x_1, y_2 + x_2, \cdots, y_n + x_n)$. When $n = 2m$, we let $LH(x) = (x_1, x_2, \cdots, x_m)$ and $RH(x) = (x_{m+1}, x_{m+2}, \cdots, x_{2m})$.

We now define the Hamming weight of an N-periodic series s as the account of nonzero elements per period of s, stated by $W_H(s)$. Suppose that s^N is one period of s. If $N = 2^n$, s^N is also stated as $s^{(n)}$. We also define the distance of two binary elements as the difference of their indexes. Precisely, for an N-periodic series $s = \{s_0, s_1, s_2, s_3, \cdots\}$, the distance of s_i, s_j, denoted as $d(s_i, s_j)$, is $j - i$, here $0 \le i \le j \le N$.

The next three lemmas on 2^n-periodical series are well known results. Please refer to [12], [16], [17] for more details.

Lemma 2.1 Let s be one periodic series of period $N = 2^n$. Then $L(s) = N$ is true if and only if the Hamming weight for a period of the binary series is odd.

Lemma 2.2 Suppose that s_1 and s_2 are two periodical series of period 2^n. If $L(s_2) \ne L(s_1)$, then $L(s_1 + s_2) = \max\{L(s_1), L(s_2)\}$; otherwise if $L(s_2) = L(s_1)$, then $L(s_2 + s_1) < L(s_1)$.

Lemma 2.3 Suppose that E_i is a 2^n-periodical series with the condition that one nonzero bit at position i and 0 elsewhere in every period, $0 \le i < 2^n$. If $j - i = 2^r(2a + 1)$, $a \ge 0$, $0 \le i < j < 2^n$, $r \ge 0$, then $L(E_i + E_j) = 2^n - 2^r$.

We have the next result on the linear complicacy of periodical series with Hamming weight less than 8.

Lemma 2.4 Let s be one periodic series of period 2^n and the Hamming weight is $w < 8$. Then the linear complicacy of s is $L(s) = 2^n - 2^{n-m}$, $1 < m \le n$ or $2^n - (2^{n-m} + 2^{n-j})$, $1 \le m < j \le n$.

In [12], the next lemma is given based on Games-Chan algorithm.

Lemma 2.5 Let s be a periodical series 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 $W_H(v)$ be the Hamming weight of a sequence v. Then the mapping φ_n has the next characters.

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

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

3) The set

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

which is the preimage of $s^{(n)}$, is of cardinality 2^{2^n}.

The next result on the account of periodical series with a given linear complicacy is presented by Rueppel [13].

Lemma **2.6** The account $N(L)$ with 2^n-periodical series of linear complicacy L, $0 \le L \le 2^n$, is presented by $N(L) = \begin{cases} 1, L = 0 \\ 2^{L-1}, 1 \le L \le 2^n \end{cases}$

In this work, we will study periodical series of linear complicacy 2^n, and periodical series of linear complicacy less than 2^n, separately. We observe that for periodical series of linear complicacy 2^n, the k-variance linear complicacy is equal to *(k + 1)*-variance linear complicacy, for k is an odd number. For periodical series of linear complicacy less than 2^n, the k-variance linear complicacy is equal to *(k + 1)*- variance linear complicacy, for k is an even number. Therefore, in order to characterize 2^n-periodical series of 4-variance linear complicacy, we need first to consider the 2^n-periodical series with linear complicacy 2^n and the 3-variance linear complicacy, and this is given in [16]. In this paper, we will fully characterize the 2^n-periodical series of linear complicacy less than 2^n and the 4-variance linear complicacy.

Similarly, in order to investigate 2^n-periodical series with the prescribed 5-variance linear complicacy, we can first consider 2^n-periodical series of linear complicacy less than 2^n and the prescribed 4-variance linear complicacy, and then we need consider 2^n-periodical series of linear complicacy 2^n and the prescribed 5-variance linear complicacy. In this paper, only partial results are given here based on the proposed main framework.

Obviously, one can extend this idea to characterize 2^n-periodical sequences of the k-variance linear complicacy when $k = 6, 7$.

We propose a structural method based on the next main framework. Let S be $\{s|L(s) = c\}$, E be $\{e|W_H(e) \le w\}$ and SE be $\{s + e|s \in S, e \in E\}$, where s is a periodic series of linear complicacy c, $w < 8$ and e is an error binary series [7] with $W_H(e) \le w$. Note that the account with 2^n-periodical series in E is $1+2^n+\binom{2^n}{2}+\cdots+\binom{2^n}{\omega}$. By Lemma 2.6, the number with 2^n-periodical series $s+e \in SE$ is at most $(1+2^n+\binom{2^n}{2}+\cdots+\binom{2^n}{\omega})2^{c-1}$. Based on the sieve approach, we want to sieve periodical $s+e$ of $L_\omega(s+e)=c$ from SE.

Intuitively, we want to characterize the 2^n-periodical sequences of linear complicacy less than 2^n and the 4-variance linear complicacy. 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 of linear complicacy less than 2^n, so we can only consider the error binary series with $W_H(e) = 0$ or 2 or 4. In the same way, when we characterize the 2^n-periodical sequences of linear complicacy 2^n and the 5-variance linear complicacy. 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 series with linear complicacy 2^n, so we can only consider the error binary sequences of $W_H(e) = 1$ or 3 or 5.

Given a 2^n-periodical series $s^{(n)}$, based on the Games-Chan algorithm [4], its linear complicacy is either 0 or $L(r, c) = 2^{n-1} + 2^{n-2} + \cdots + 2^r + c = 2^n - 2^r + c$, $1 \le c < 2^{r-1}$, $2 \le r \le n$. With the next result, we only need to consider 2^r-periodical series $s^{(r)}$ with *linear complicacy* c.

Lemma 2.7 Let $s^{(n)}$ be one periodical series of period 2^n and its linear complicacy be either 0 or $L(r, c) = 2^{n-1} + 2^{n-2} + \cdots + 2^r + c = 2^n - 2^r + c$, $1 \le c \le 2^{r-1} - 1$, $2 \le r \le n$. Let $u^{(r)}$ be a periodical series with period 2^r and $W_H(u^{(r)}) = k$, and $u^{(n)}$ be a periodical series 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 $s^{(r)} = \varphi_{r+1} \cdots \varphi_n(s^{(n)})$.

By Lemma 2.7, in order to study 2^n-periodical sequences of the k-variance linear complicacy, we just need to consider the k-variance linear complicacy for $0 \le c < 2^{n-1}$. For such purpose, we first study a simple case.

Lemma **2.8** Let series $s^{(n)}$ and series $t^{(n)}$ be different but of the same linear complicacy c, $1 \le c \le 2^{n-3}$, and $u^{(n)}$ and $v^{(n)}$ be two different periodical series with $W_H(u^{(n)}) < 8$, $W_H(v^{(n)}) < 8$. Then $t^{(n)} + v^{(n)} \ne s^{(n)} + u^{(n)}$.

Now we need to consider more complicated cases with linear complicacy $2^{n-3} < c < 2^{n-1}$. First we have the next result.

Lemma **2.9** 1). Let $s^{(n)}$ be one periodical series of linear complicacy c, $1 \le c \le 2^{n-1} - 3$, $c \ne 2^{n-1} - 2^{n-m}$, $1 < m < n - 1$ and $c \ne 2^{n-1} - (2^{n-m} + 2^{n-j})$, $1 < m < j \le n$; $u^{(n)}$ be one periodical series of $W_H(u^{(n)}) \le k$, $4 \le k < 8$. Then the k-variance linear complicacy of $s^{(n)} + u^{(n)}$ is still c.

2). Let $s^{(n)}$ be a periodical series with linear complicacy $c = 2^{n-1} - 2^{n-m}$, $1 < m \le n$ or $c = 2^{n-1} - (2^{n-m} + 2^{n-j})$, $1 < m < j \le n$. Then there exists a periodical series $u^{(n)}$ with $W_H(u^{(n)}) \le k$, $4 \le k < 8$, so that the k-variance linear complicacy of $s^{(n)} + u^{(n)}$ is less than c.

Now by Lemma 2.9, we need only to consider the next three cases. i) $c = 2^{n-1} - 2^{d_1} - 2^{d_2}, 0 \le d_2 < d_1 \le n - 2$.

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

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

For a given linear complicacy c, now it remains only for us to study two situations. One case is that $s+u \in SE$, however $L_W(s+u) < c$. This is equal to verifying whether there exists a periodical series v with the condition 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 SE. The other case is that $s+u, t+v \in SE$ and $L_W(s+u) = L_W(s+v) = c$ with the condition that $s \neq t, u \neq v$, however $s+u=t+v$. It is equal to verifying whether there exists a periodical series v with the condition that $L(s+t)=L(u+v)<c$ and if so, calculate the account of such periodical series v, where $W_H(u) \le w$, $W_H(v) \le w$. 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 SE. Throughout this paper, this technique will be used in different places.

In next section, we will fully characterize the 4-variance linear complicacy distribution with 2^n-periodical series of linear complicacy less than 2^n.

3. Calculating Formulas for the 4-Variance Linear Complicacy

In [16], the 3-variance linear complicacy with 2^n-periodical series of linear complicacy 2^n has been investigated. For 2^n-periodical series of linear complicacy 2^n, the change of 4 bits each period will result in a periodical series with an odd number of nonzero bits for each period, hence still with linear complicacy 2^n. Therefore, the 4-variance linear complicacy is equivalent to the 3-variance linear complicacy with 2^n-periodical series in the case of linear complicacy 2^n. To investigate the calculating formulas for the 4-variance linear complicacy with 2^n-periodical series in general, we only need to obtain the calculating formulas for the 4-variance linear complicacy with 2^n-periodical series of linear complicacy less than 2^n. To this end, we put the 4-variance linear complicacy into six non trivial categories and process them respectively.

We first consider the category for periodical series of 4-variance linear complicacy $2^{n-2} - 2^{n-m}$. As $2^{n-2} - 2^{n-m} = 2^{n-1} - 2^{n-2} - 2^{n-m}$, so this is a special case of i).

Lemma **3.1** Suppose that $N_4(2^{n-2} - 2^{n-m})$ is the number with 2^n-periodical series for linear complicacy less than 2^n and 4-variance linear complicacy $2^{n-2} - 2^{n-m}, 2 < m \le n, n > 2$. 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

$$C1 = 2^{n+m-6}\binom{8}{4} - 2^{n-2}\left(2^{m-3} - 1\right)$$

$$C2 = \sum_{k=3}^{m-1} 2^{n+k-6}\left(\binom{8}{4} - 2\right) = \left(2^{n+m-6} - 2^{n-3}\right)\left(\binom{8}{4} - 2\right)$$

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

Lemma **3.2** Suppose that $N_4(2^{n-2} - 2^{n-m} + x)$ is the account with 2^n-periodical binary series for *linear complicacy less than* 2^n and 4-variance linear complicacy $2^{n-2} - 2^{n-m} + x, n > 4, 0 < x < 2^{n-m-1}, 2 < m < n-1$. Then

$$N_4(2^{n-2}-2^{n-m}+x)=\left[1+\binom{2^n}{2}+\binom{2^n}{4}-2^{n-3}+2^{n-m}-\frac{1}{2}(C1+C2)\right]\times 2^{2^{n-2}-2^{n-m}+x-1}$$

where *C1, C2* are defined in Lemma 3.1.

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 periodical series for 4-variance linear complicacy $2^{n-1}-2^{n-m}$.

Lemma **3.3** Suppose that $N_4(2^{n-1}-2^{n-m})$ is the account with 2^n-periodical series for *linear complicacy less than* 2^n and 4-variance linear complicacy $2^{n-1}-2^{n-m}, 2\le m\le n$. Then

$$N_4(2^{n-1}-2^{n-m})=\left[E8/8+E6/6-E7+E4/2-E5+E2/4-E3+\binom{2^n}{4}-E1\right]\times 2^{2^{n-1}-2^{n-m}-1}$$

where

$$E1=\binom{2^{n-m}}{2}\times\binom{2^m}{2}\times\binom{2^m}{2}$$

$$E2=4\times\binom{2^{n-m}}{2}\times\binom{2^{m-1}}{2}\times\binom{2^{m-1}}{2}-\binom{2^{n-m}}{2}\times\left[2^{2m-2}+2^{m+1}\left(\binom{2^{m-1}}{2}-2^{m-2}\right)\right]$$

$$E3=\binom{2^{n-m}}{3}\times\binom{3}{1}\times\binom{2^m}{2}\times 2^m\times 2^m$$

$$E4=\binom{2^{n-m}}{3}\binom{3}{1}\binom{2^{m-1}}{2}\times 2^{2m+1}-\binom{2^{n-m}}{3}\binom{3}{1}\times 2^{3m-1}$$

$$E5=\binom{2^{n-m}}{3}\binom{2}{1}\binom{2^m}{3}\times 2^m$$

$$E6=2^{m+2}\times\binom{2^{n-m}}{2}\times\binom{2^{m-1}}{3}-\binom{2^{n-m}}{2}\times\left(2^{m-1}-2\right)\times 2^{2m}, E7=2^{n-m}\times\binom{2^m}{4}$$

$$E8=2^{n-m+1}\times\binom{2^{m-1}}{4}-\left[2^{n-1}\times\binom{2^{m-1}-2}{2}-2^{n-m+1}\times\binom{2^{m-2}}{2}\right]$$

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 **3.4** Let $s^{(n)}$ be a 2^n-periodic series of linear complicacy $2^{n-1}-(2^{n-m}+2^{n-j})$, $2<m<j\le n$, $n>3$, and $W_H(s^{(n)})=8$. Then the account of these series $s^{(n)}$ is $2^{n+2m+j-10}$.

Now it is time to study the category of periodical series for 4-variance linear complicacy $2^{n-1}-(2^{n-m}+2^{n-j})$.

In order to simplify the complicacy of the proof of Lemma 3.5 in this case, we first analyze the possible decompositions and then give an outline for its proof.

It remains for us to investigate two cases. Case A is to exclude all periodical series $s + u$ satisfying $s+u \in SE$, but $L_4(s+u) < 2^{n-1} - (2^{n-m} + 2^{n-j})$. Based on Lemma 2.2, this is equal to verifying whether there exists a binary series v with the condition 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 binary series in SE satisfying that $s + u, t + v \in SE$ and $L_4(s + u) = L_4(t + v) = 2^{n-1} - (2^{n-m} + 2^{n-j})$ with $s \neq t$, $u \neq v$, however $s + u = t + v$. Similarly, this is equal to verifying whether there exists a binary series v so that $L(u+v) = L(s+t) < 2^{n-1} - (2^{n-m} + 2^{n-j})$ and if so, check the account of such periodical binary series . This is the first layer decomposition in Figure 3.1.

In Case A, we need to investigate the account of periodical series $w^{(n)}$ with the condition that $w^{(n)} = u^{(n)} + v^{(n)}$ 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 account of $w^{(n)}$, we need to derive the account 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 2 nonzero bits with distance 2^{n-1} among 4 nonzero bits of $u^{(n)}$. This is the decomposition under node A in Figure 3.1.

In Case B, there are also two subcases. Case B.1: we need to first find the account of periodical series $w^{(n)}$ with the condition that $w^{(n)} = u^{(n)} + v^{(n)}$ 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 periodic series $u^{(n)}$ for which there is no periodical binary series $v^{(n)}$, so that $L(v^{(n)} + u^{(n)}) = 2^{n-1} - (2^{n-m} + 2^{n-k})$, $m < k < j$. This is the decomposition under node B in Figure 3.1.

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 bits with distance 2^{n-1} among 4 nonzero bits of $u^{(n)}$. Case B.1.3: There are no 2 nonzero bits with distance 2^{n-1} among 4 nonzero bits 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 account of periodical series $u^{(n)}$ in all the nodes and there are total 10 leaves (cases). These cases are investigated one by one in Lemma 3.5.

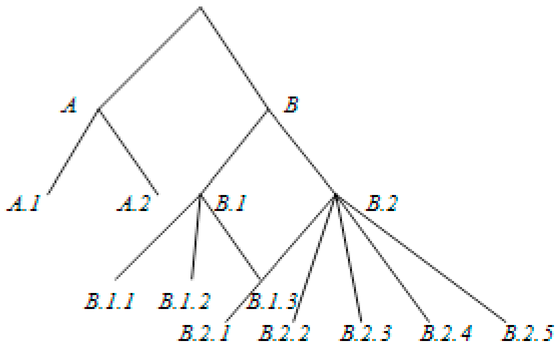

Fig.3.1 The decomposition of series with $L_4(s + u) = 2^{n-1} - (2^{n-m} + 2^{n-j})$

Next we will deal with all the cases in Fig.3.1 in Lemma 3.5.

Lemma **3.5** Suppose that $N_4(2^{n-1} - 2^{n-m} - 2^{n-j})$ is the account of 2^n-periodical series for linear complicacy less than 2^n and 4-variance linear complicacy $2^{n-1} - 2^{n-j} - 2^{n-m}$, $2 < m < j \leq n, n > 3$. Then

$N_4(2^{n-1} - 2^{n-m} - 2^{n-j})$

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

where

$$F4 = 2^{n+2m+j-6} + 2^{n+m-4} + 2^{n+j-4} + 3 \times 2^{n+m+j-4}$$

$$F6 = 2^{n+k-4},\ F7 = 3 \times 2^{n+m+k-4},\ F8 = 2^{n+2m+k-6}$$

$$F10 = 2^{n-1},\ F11 = 2^{n-m+1}\binom{2^{m-1}}{2} - 2^{n-1}$$

$$F13 = \binom{2^{n-m+1}}{2} \times 2^{2m-2} \times \left(2^{m-1} - 2\right)$$

$$F14 = \binom{2^{n-m+1}}{2} \times \binom{2^{m-1}}{3} \times 2^{m} - \binom{2^{n-m+1}}{2} \times 2^{2m-2} \times \left(2^{m-1} - 2\right)$$

$$F17 = \binom{2^{n-m+1}}{2} \times 2^{m-1} - \left[\binom{2^{m-1}}{2} - 2^{m-2}\right]$$

$$F18 = \binom{2^{n-m+1}}{2} \times \left[\binom{2^{m-1}}{2} - 2^{m-2}\right]^2$$

$$F22 = \binom{2^{n-m+1}}{3}\binom{3}{1} \times \left[\binom{2^{m-1}}{2} - 2^{m-2}\right] \times \left(2^{m-1}\right)^2$$

$$F19 = \binom{2^{n-m+1}}{2} \times \binom{2^{m-1}}{2}^2 - \sum_{k=m}^{j} 2^{n+k-4} - \binom{2^{n-m+1}}{2} \times 2^{m-1} \times \left[\binom{2^{m-1}}{2} - 2^{m-2}\right] - \binom{2^{n-m+1}}{2} \times \left[\binom{2^{m-1}}{2} - 2^{m-2}\right]^2$$

$$F23 = 3\binom{2^{n-m+1}}{3} \times 2^{3m-4} - 3\sum_{k=m+1}^{j} 2^{n+m+k-4}$$

$$F25 = 2^{n-m+1} \times \binom{2^{m-2}}{2},\ F26 = 2^{n-1} \times \left[\binom{2^{m-1}-2}{2} - \left(2^{m-2}-1\right)\right]$$

$$F27 = 2^{n-m+1}\left\{\binom{2^{m-1}}{4} - \binom{2^{m-2}}{2} - 2^{m-2} \times \left[\binom{2^{m-1}-2}{2} - \left(2^{m-2}-1\right)\right]\right\}$$

Let us denote $N_4\left(2^{n-1} - \left(2^{n-m} + 2^{n-j}\right)\right) = p(n, m, j) \times 2^{2^{n-1}-\left(2^{n-m}+2^{n-j}\right)-1}$ with notation $p(n,m,j)$. Now we investigate the category of periodical series with 4-variance linear complicacy $2^{n-1} - 2^{n-m} - 2^{n-j} + x$.

Lemma **3.6** Suppose that $N_4(2^{n-1}-2^{n-m}-2^{n-j}+x)$ is the account with 2^n-periodical series for *linear* complicacy *less than* 2^n and 4-variance linear complicacy $2^{n-1}-2^{n-m}-2^{n-j}+x$, $n>5$, $2<m<j<n-1$, $1\le x<2^{n-j-1}$. Then

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

where $F6,F7,\cdots,F27$ are defined in Lemma 3.5.

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

Lemma **3.7** Suppose that $L(r,c)=2^n-2^r+c$, $1\le c\le 2^{r-3}-1$, $4\le r\le n$, and $N_4(L)$ is the account with 2^n-periodical sequences for *linear complicacy less than* 2^n and 4-variance linear complicacy L. Then

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

Now by summarizing all the results above and using the technique of extending the period from 2^r to 2^n used in Lemma 3.7, we could have the next important theorem.

Theorem **3.1** Suppose that $L(r,c)=2^n-2^r+c$, $1\le c\le 2^{r-1}-1$, $2\le r\le n$, and $N_4(L)$ is the account of 2^n-periodical series for linear complicacy less than 2^n and 4-variance linear complicacy L. Then

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

where $f(r,m)$, $g(r,m)$, $h(r,m)$, $p(r,m,j)$, $q(r,m,j)$ are defined in Lemma 3.1, 3.2, 3.3, 3.5 and 3.6 respectively.

For $n = 5$, we have verified the numbers with 2^n-periodical sequences for linear complicacy less than 2^n and the 4-variance linear complicacy c, $0 \le c < 2^n$, with a computer program. The lengthy results are omitted here due to space limitation.

4. Conclusions

In this paper, we used the same framework proposed in [16] and completely solved the problem of the 4-variance linear complicacy distribution for 2^n-periodical series. In comparison of the results and proofs in this paper and [16], one can see that the decomposition in this paper is much more complicated though the same framework is adopted. In other words, the applicability of the proposed main framework in [16] is validated for solving more complicated problem in this paper. With combination of results in [16], we completely solve the problem of the calculating function distributions of 4-variance linear complicacy for 2^n-periodical series elegantly, which very significantly improves the results in the relating references.

Of course, we can consider the 5-variance linear complicacy, the 6-variance linear complicacy and the 7-variance linear complicacy with the proposed approach in this paper and obtain some partial results. As to the importance 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.

References

1. Ding CS. *Lower bounds on the weight complexity of cascaded binary sequences*. In: Proc. of Auscrypt'90, Advances in Cryptology, LNCS 453, Springer-Verlag; 1990, p.39-43.
2. Ding, CS, Xiao, GZ, Shan, WJ. *The stability theory of stream ciphers*. Germany: Springer-Verlag; 1991.
3. Etzion T, Kalouptsidis N, Kolokotronis N, Limniotis K, Paterson KG. Properties of the Error Linear Complexity Spectrum. *IEEE Transactions on Information Theory* 2009; **55**: 4681-6.

4. Games, RA, Chan, AH. A fast algorithm for determining the complexity of a binary sequence with period 2n. IEEE Trans on Information Theory 1983; 29:144-2.
5. Fu F, Niederreiter H, and Su M. The characterization of 2n-periodic binary sequences with fixed 1-error linear complexity. In: Gong G., Helleseth T, Song HY, Yang K. (eds.) SETA 2006, LNCS, 4086, Springer; 2006, p. 88-103.
6. Han YK, Chung JH, Yang K. On the k-error linear complexity of pm-periodic binary sequences. IEEE Transactions on Information Theory 2007; 53: 2297-7.
7. Kaida T, Uehara S, Imamura K. An algorithm for the k-error linear complexity of sequences over GF(pm) with period pn, p a prime. Information and Computation 1999; 151:134 -4.
8. Kavuluru R. Characterization of 2n-periodic binary sequences with fixed 2-error or 3-error linear complexity, Des Codes Cryptogr 2009; 53: 75-23.
9. Kurosawa K, Sato F, Sakata T, Kishimoto W. A relationship between linear complexity and k-error linear complexity. IEEE Transactions on Information Theory 2000; 46: 694-5.
10. Lauder A, Paterson K. Computing the error linear complexity spectrum of a binary sequence of period 2n. IEEE Transactions on Information Theory 2003; 49: 273-8.
11. Meidl W. How many bits have to be changed to decrease the linear complexity? Des Codes Cryptogr 2004; 33: 109-4.
12. Meidl W. On the stablity of 2n-periodic binary sequences. IEEE Transactions on Information Theory 2005; 51: 1151-5.
13. Rueppel RA. Analysis and design of stream ciphers. Berlin: Springer-Verlag; 1986; chapter 4.
14. Stamp M, Martin CF. An algorithm for the k-error linear complexity of binary sequences with period 2n. IEEE Trans Inform Theory 1993; 39: 1398-4.
15. Xiao GZ. Wei SM, Lam KY, Imamura K. A fast algorithm for determining the linear complexity of a sequence with period pn over GF (q). IEEE Trans on Information Theory 2000; 46: 2203-4.
16. Zhou JQ, Liu WQ. The k-error linear complexity distribution for 2n-periodic binary sequences. Des Codes Cryptogr 2014; 73:55-3.
17. Zhu FX, Qi WF. The 2-error linear complexity of 2n-periodic binary sequences with linear complexity 2n-1. Journal of Electronics (China) 2007; 24: 390-6.