On the Generalized Lauder-Paterson Algorithm and Profiles of the k-Error Linear Complexity for Exponent Periodic Sequences

Takayasu Kaida

Department of Information and Electronic Engineering,
Yatsushiro National College of Technology,
Yatsushiro, Kumamoto 866-8501, Japan
kaida@m.ieice.org, kaida@as.yatsushiro-nct.ac.jp
http://y-page.yatsushiro-nct.ac.jp/u/kaida/index.html

Abstract. The Lauder-Paterson algorithm gives the profile of the k-error linear complexity for a binary sequence with period 2^n. In this paper a generalization of the Lauder-Paterson algorithm into a sequence over $GF(p^m)$ with period p^n, where p is a prime and m, n are positive integers, is proposed. We discuss memory and computation complexities of proposed algorithm. Moreover numerical examples of profiles for balanced binary and ternary exponent periodic sequences, and proposed algorithm for a sequence over $GF(3)$ with period $9(= 3^2)$ are given.

Keywords: exponent periodic sequence, Games-Chan algorithm, k-error linear complexity, Lauder-Paterson algorithm, pseudo-random sequence, Stamp-Martin algorithm.

1 Introduction

In 1993 M.Stamp and C.Martin proposed the k-error linear complexity (k-LC) for periodic sequences as one of measurements for randomness [10]. The k-LC is a generalization of the linear complexity (LC) in order to guard from instability properties of the LC [11, 12, 1]. At the same time a fast algorithm (Stamp-Martin algorithm) of the k-LC for a binary sequence with period 2^n is shown [10]. Although the sphere complexity, as similar as the k-LC, was proposed earlier than the k-LC [2], we use the k-LC in sense of a natural extension of the LC. We generalized the Stamp-Martin algorithm into two algorithms for a sequence over $GF(p^m)$ with period p^n, where p is a prime and m, n are positive integers [4, 5]. One of them should be called the generalized Stamp-Martin algorithm because this algorithm becomes the Stamp-Martin algorithm in case of binary sequences [5]. Another one has the same function and does not use concepts named "shift" and "offset" [4]. The procedure of "shift" changes the cost matrix to fit the input sequence at that step by the cyclic shift for each columns of the cost matrix. After this, all elements of the value at the first row are same value and the minimum through all elements of that shifted cost matrix. Therefore we can set

T. Helleseth et al. (Eds.): SETA 2004, LNCS 3486, pp. 166–178, 2005.

all-zero at the first row by subtracting that value from all elements of the cost matrix, called the procedure of "offset". For binary sequences, "shift" and "offset" are very effective because these work for changing the cost matrix into the cost vector, and decreasing input value k. However in non-binary case, there is not so much benefits only dropping one row of the cost matrix. In calculations of the k-LC for non-binary exponent periodic sequences, the algorithm without "shift" and "offset" is simpler than the generalized Stamp-Martin algorithm with "shift" and "offset". It is important for applications that a pseudorandom sequence has good profile of the k-LC, which is the decrease points of the k-LC against increase of k [2, 8, 6]. Unfortunately, the Stamp-Martin algorithm and two generalized Stamp-Martin algorithms answer the k-LC against only one fixed k and one fixed binary sequence with period 2^n or one fixed sequence over $GF(p^m)$ with period p^n, respectively. Recently A.Lauder and K.Paterson proposed a fast algorithm (Lauder-Paterson algorithm) computing the profile of the k-LC, i.e., the k-LC for all $k \geq 0$, for a fixed binary sequence with period 2^n [9].

In this paper the LC and its fast algorithm such as the generalized Games-Chan algorithm, and the k-LC and the generalized k-LC algorithm are recalled in Section 2 and Section 3, respectively. For preliminaries of a generalization of the Lauder-Paterson algorithm, we describe the profiles of the k-LC and the Lauder-Paterson algorithm in Section 4. The main theorem and proposed generalized Lauder-Paterson algorithm for a sequence over $GF(p^m)$ with period p^n are given in Section 5. Because of complications in the algorithm with "shift" and "offset", we propose the generalized Lauder-Paterson algorithm without "shift" and "offset" although the original Lauder-Paterson algorithm uses "shift" and "offset". In Section 6 some numerical examples for profiles for balanced binary and ternary exponent periodic sequences, and proposed algorithm for a sequence over $GF(3)$ with period $9(= 3^2)$ are given. Finally conclusion and future works are shown in Section 7.

2 Linear Complexity and Generalized Games-Chan Algorithm

We define the linear complexity of a sequence and recall the generalized Games-Chan algorithm [3, 2] computing the LC for a sequence over $GF(p^m)$ with period p^n.

We consider an infinite sequence $S = (s_0, s_1, \cdots)$ over a finite field K through this paper.

Definition 1. *The linear complexity (LC) of S is defined as*

$$L(S) = \min\{\deg f(x) | f(x) \in G(S)\},$$

where the set $G(S)$ consists of the generator polynomial,

$$f(x) = f_L x^L + f_{L-1} x^{L-1} + \cdots + f_1 x + 1 \in K[x],$$

of S such that

$$s_{L+i} + f_1 s_{L+i-1} + \cdots + f_{L-1} s_{i+1} + f_L s_i = 0 \tag{1}$$

for all integer $i \geq 0$. □

Definition 2. *If there exists an integer N such that $s_i = s_{N+i}$ for all $i \geq 0$ then N is defined the period of S.* □

In this paper we call the period of S only the minimum of N satisfying above condition the period of S.

We denote one period (or subsequence) with length N of an infinite sequence S by $S^{(N)}$, i.e., $S^{(N)} = (s_0, s_1, \cdots, s_{N-1})$, and an infinite sequence repeating a finite sequence F by F^∞. Hence we can rewrite an infinite sequence S with period N by $S = (S^{(N)})^\infty$.

The LC can be also defined for a finite sequence with length N by satisfying (1) for $0 \leq i \leq N - L$ instead of all $i \geq 0$. However we only consider the LC of infinite sequences in this paper then let F be a finite sequence, we simply denote $L(F)$ and $L_k(F)$ instead of $L(F^\infty)$ and $L_k(F^\infty)$, respectively. ($L_k(F)$ will be defined in next section.)

Definition 3. *Let $K = GF(p^m)$ with a prime p and a positive integer m. If a sequence S over K has the period $N = p^n$ with a positive integer n then S is called an exponent periodic sequence.* □

For exponent periodic sequences the generalized Games-Chan algorithm is known as one of fast algorithms computing the LC.

Definition 4. *For an exponent periodic sequence S over $K = GF(p^m)$ with period $N = p^n = pM$, we define one period of S by*

$$S^{(N)} = (\boldsymbol{s}(0)^{(M)}, \boldsymbol{s}(1)^{(M)}, \cdots, \boldsymbol{s}(p-1)^{(M)}),$$

i.e., $\boldsymbol{s}(j)^{(M)} = (s_{jM}, s_{jM+1}, \cdots, s_{(j+1)M-1})$ for $0 \leq j < p$ and a vector $\boldsymbol{b}^{(M,u)}$ with length M over K is defined by

$$\boldsymbol{b}^{(M,u)} = F_u(\boldsymbol{s}(0)^{(M)}, \boldsymbol{s}(1)^{(M)}, \cdots, \boldsymbol{s}(p-1)^{(M)}) \tag{2}$$

for $0 \leq u < p$, where

$$F_u(\boldsymbol{s}) = \sum_{j=0}^{p-u-1} \binom{p-j-1}{u} s_j \tag{3}$$

of $\boldsymbol{s} = (s_0, s_1, \cdots, s_{p-1}) \in K^p$ is applied componentwise and $\binom{p-j-1}{u}$ means the binomial coefficients of $p-j-1$ and u. □

We recall the generalized Games-Chan algorithm shown in Fig.1. It is obvious that the generalized Games-Chan algorithm is induced by Definition 4. The final L of the generalized Games-Chan algorithm indicates the LC of an infinite sequence S with its one period $S^{(N)}$.

```
input: S^(N) = (s_0, s_1, ..., s_{N-1}), N = p^n
M = p^{n-1}, L = 0, s^(N) = S^(N),
for j = n - 1 down to 0
    b^(M,u) for 0 ≤ u ≤ p - 2 from s^(pM) by (2)
    if b^(M,0) ≠ 0 then case 1
    if b^(M,u) = 0 for 0 ≤ u ≤ w - 2, b^(M,w-1) ≠ 0 then case w
    if b^(M,u) = 0 for 0 ≤ u ≤ p - 2 then case p
    if case w then s^(M) = b^(M,w-1) from (2) and L = L + (p - w)M
    if M ≠ 1 then M = M/p
if s_0^(1) ≠ 0 then L = L + 1
```

Fig. 1. Generalized Games-Chan algorithm

3 *k*-Error Linear Complexity and Generalized *k*-LC Algorithm

In this section the k-LC and the generalized k-LC algorithm (see Fig.2) is also recalled in order to derive a generalization of the Lauder-Paterson algorithm.

Definition 5. *The k-error linear complexity (k-LC) of a periodic sequence S over K with period N is defined as*

$$L_k(S) = \min\{LC(S+E) | W(E^{(N)}) \leq k\},$$

where a periodic sequence E over K has period N or the divisor of N, $W(E^{(N)})$ is the Hamming weight of $E^{(N)} = (e_0, e_1, \cdots, e_{N-1})$ and a sequence $S + E = (s_0 + e_0, s_1 + e_1, \cdots)$ over K. □

We have $L_{k-1}(S) \geq L_k(S)$ for $1 \leq k \leq W = W(S^{(N)})$, $L_0(S) = L(S)$ and $L_k(S) = 0$ for $W \leq k \leq N$ from Definition 5 obviously.

If a sequence S is an exponent periodic sequence then we can apply the generalized k-LC algorithm to S.

Definition 6. *Let a sequence S be an exponent periodic sequence over $K = GF(p^m)$ with period $N = p^n$ and a $q \times N$ matrix $\Sigma = [\sigma(h, i)]$ for $1 \leq h \leq q$, $0 \leq i < N$ over the integers, where $q = p^m$, and Σ is called a cost matrix of S. Moreover let α be a primitive element over K. We need that h-th row of Σ ($1 \leq h \leq q$) corresponds to an element α_h in K, then we set $\alpha_1 = 0$ and $\alpha_h = \alpha^{h-2}$ for $2 \leq h \leq q$.* □

When the initial cost matrix $\Sigma = [\sigma(h, i)]$ is defined as

$$\sigma(h, i) = \begin{cases} 0 \text{ if } h = 1, \\ 1 \text{ if } h \neq 1 \end{cases} \tag{4}$$

for $1 \leq h \leq q, 0 \leq i < N$, an element $\sigma(h, i)$ of the cost matrix Σ indicates the number of changing element at the original sequence with length N for

substituting $s_i^{(M)}$ into $s_i^{(M)} + \alpha_h$ at that depth with length M and keeping the final LC by a previous depth.

From the generalized Games-Chan algorithm we need to set ranges of the LC. At the step M, meaning its input sequence with length pM, the value $T^{(M,u)}$, defined in next definition, means the minimum changing number of the LC range increasing LC value from $(p-w-1)M$ up to $(p-w)M$, and the set $D_i^{(M,u)}$ consists of all error pattern collecting error values at position $i, M+i, \ldots, (p-1)M+i$ at its input sequence with length pM satisfying above condition.

Definition 7. *Let a sequence S be an exponent periodic sequence over $K = GF(p^m)$ with period $N = p^n$ and a $q \times N$ matrix $\Sigma^{(N)}$, and let $M = N/p = p^{n-1}$. For $0 \le u < p-1$*

$$T^{(M,u)} = \sum_{i=0}^{M-1} B_i^{(M,u)} \tag{5}$$

is calculated from S and $\Sigma^{(N)} = [\sigma(h,i)^{(N)}]$ by

$$B_i^{(M,u)} = \min \left\{ \sum_{j=0}^{p-1} \sigma(h_j, jM+i) \,\middle|\, \boldsymbol{e} \in D_i^{(M,u)} \right\}$$

for $0 \le i < M$, where $\boldsymbol{e} = (\alpha_{h_0}, \alpha_{h_1}, \cdots, \alpha_{h_{p-1}}) \in K^p$ and

$$D_i^{(M,u)} = \{\boldsymbol{e} | F_j(\boldsymbol{e}) + b_i^{(M,j)} = 0 \ (0 \le j \le u)\}$$

from (2) and (3). □

Next calculations of the cost matrix $\Sigma_w^{(M)}$ for next step by case w, its input sequence with length M, in the generalized k-LC algorithm are defined as follows:

Definition 8. *Let a sequence S be an exponent periodic sequence over $K = GF(p^m)$ with period $N = p^n$ and a $q \times N$ matrix $\Sigma^{(N)}$, and let $M = N/p = p^{n-1}$. Then $\Sigma_w^{(M)} = [\sigma(h,i)_w^{(M)}]$ is calculated from S and $\Sigma^{(N)}$ by*

$$\sigma(h,i)_w^{(M)} = \min \left\{ \sum_{j=0}^{p-1} \sigma(h_j, jM+i)^{(N)} \,\middle|\, \boldsymbol{e} \in \hat{D}(h,i)_w^{(M)} \right\}, \tag{6}$$

where $\boldsymbol{e} = (\alpha_{h_0}, \alpha_{h_1}, \cdots, \alpha_{h_{p-1}}) \in K^p$ and

$$\hat{D}(h,i)_1^{(M)} = \{\boldsymbol{e} \in K^p | F_0(\boldsymbol{e}) - \alpha_h = 0\},$$
$$\hat{D}(h,i)_w^{(M)} = \left\{ \boldsymbol{e} \in K^p \,\middle|\, \begin{array}{l} F_j(\boldsymbol{e}) + b_i^{(M,j)} = 0 \ (0 \le j < w-1), \\ F_{w-1}(\boldsymbol{e}) - \alpha_h = 0 \end{array} \right\}$$

for $2 \le w \le p$. □

These calculations propagate information about the number of change at the original input sequence with length N from step M to step M/p.

After above preparations, we show the generalized k-LC algorithm of the k-LC without shift and offset in Fig.2. The final value L of this algorithm is the k-LC with a fixed k of its input exponent periodic sequence S. This algorithm and the Lauder-Paterson algorithm, shown in next section, are used for proposed generalization of the lauder-Paterson algorithm.

---

input: k, $S^N = (s_0, s_1, \cdots, s_{N-1})$, $N = p^n$

$M = p^{n-1}$, $L = 0$, $\boldsymbol{s}^{(N)} = S^N$,

$\Sigma^{(N)} = [\sigma(h,i)^{(N)}]$, $\sigma(h,i)^{(N)} = \begin{cases} 0, \text{ if } h = 1, \\ 1, \text{ if } h \neq 1 \end{cases}$

for $j = n-1$ **down to** 0

  $T^{(M,u)}$ for $u = 0, \cdots, p-2$ from (5)

  if $k < T^{(M,0)}$ **then** case 1

  if $T^{(M,w-2)} \leq k < T^{(M,w-1)}$ **then** case w

  if $T^{(M,p-2)} \leq k$ **then** case p

  if case w **then** $\boldsymbol{s}^{(M)} = \boldsymbol{b}^{(M,w-1)}$ from (2) and $L = L + (p-w)M$

  Set $\Sigma^{(M)} = \Sigma_w^{(M)}$ from $\Sigma^{(pM)}$ by (6)

  if $M \neq 1$ **then** $M = M/p$

if $\sigma(h,0) > k$ **such that** $\alpha_h - s_1^{(0)} = 0$ **then** $L = L + 1$

Fig. 2. Generalized k-LC algorithm

4 Profile of k-LC and Lauder-Paterson Algorithm

In this section we recall the profile of the k-LC and the Lauder-Paterson algorithm. The Lauder-Paterson algorithm, which gives the profile of the k-LC for a binary exponent sequence with period 2^n, is shown in Fig.3.

Definition 9. *Let a triple $\hat{S} = (S, \sigma, N)$ with a binary sequence S with length N, a vector σ over the integers*[1] *with length N and $N = 2^n$ be a cost binary sequence. We define $B(\hat{S}) = (B(S), B(\sigma), N/2)$ with length $N/2$ by*

$$B(S)_i = s_i + s_{i+(N/2)},\ B(\sigma)_i = \min\{\sigma_i, \sigma_{i+(N/2)}\}$$

for $0 \leq i < N/2$. And $L(\hat{S}) = (L(S), L(\sigma), N/2)$ with length $N/2$ is defined by

$$L(S)_i = \begin{cases} s_i \text{ if } s_i = s_{i+(N/2)} \text{ or } \sigma_i > \sigma_{i+(N/2)}, \\ s_{i+(N/2)} \text{ otherwise}, \end{cases}$$
$$L(\sigma)_i = \begin{cases} \sigma_i + \sigma_{i+(N/2)} & \text{if } s_i = s_{i+(N/2)}, \\ |\sigma_i - \sigma_{i+(N/2)}| & \text{otherwise} \end{cases} \tag{7}$$

for $0 \leq i < N/2$, where $|a|$ is the absolute value of a. □

[1] The vector σ is originally defined over real numbers [9]. However σ is enough to over integers in this paper.

```
   input: LP(Ŝ, t, r, c)
if ℓ > 1 then
   T = Σ_{B(S)_i=1} B(σ)_i for i = 0 to ℓ/2 − 1
   if T > 0 then LP(B(Ŝ), t, min{r, t + T − 1}, c + (ℓ/2))
   if t + T ≤ r then LP(L(Ŝ), t + T, r, c)
else   /* ℓ = 1 */
   if s_0 = 0 then output (t, c)
   if s_0 = 1 and σ_0 > 0 then output (t, c + 1)
   if s_0 = 1 and t+σ_0 ≤ r then output (t+σ_0, c)
```

Fig. 3. Lauder-Paterson algorithm

The Lauder-Paterson algorithm is a recurrent algorithm (see Fig.3) and its final output from the initial input $\mathtt{LP}(\hat{S} = (S^{(N)}, \sigma = (1, 1, \cdots, 1), N), 0, N, 0)$ is equal to the extended decrease set $EDS(S)$, defined by

$$EDS(S) = \{(0, L(S))\} \cup \left\{(k, L_k(S)) \,\middle|\, L_k(S) < L_{k-1}(S), 1 \le k \le W\left(S^N\right)\right\}$$

for an exponent periodic sequence S with period $N = 2^n$. From the definition of the k-LC, $EDS(S)$ shows complete profile of the k-LC for a cost binary sequence $\hat{S}$ with period 2^n.

5 Generalization of Lauder-Paterson Algorithm

In this section we propose a generalized Lauder-Paterson algorithm (see Fig.4) which is not used the concepts of shift and offset as same as the generalized k-LC algorithm proposed in [4], although the Lauder-Paterson algorithm is using them as same as the Stamp-Martin algorithm [10] and its second generalization [5].

We can construct proposed algorithm as same as the Lauder-Paterson algorithm which is a recurrent algorithm. we need to consider p branches in each depth and some conditions are decided by their cost matrix in similar to the generalized Games-Chan algorithm. Moreover from the generalized k-LC algorithm and Definition 5 (the definition of the k-LC), for instance, if $r = T^{(M,0)}$ or $T^{(M,w-1)} = T^{(M,w)}$ or $T^{(M,p-2)} = t$ in case of $p = 3$ then there is no decrease point in the corresponding range decided the k-LC. Next main theorem is derived from above discussion.

Theorem 1. *Let $(S^{(N)}, \Sigma, N, 0, 0, N + 1)$ be an input of the generalized Lauder-Paterson algorithm shown in Fig.4, where $\Sigma = [\sigma(h, i)]$ is defined from (4). The final output of the algorithm indicates the extended decrease set $EDS(S)$ of an exponent periodic sequence S with period N.*

(**Sketch of Proof**)**:** At first calculations of borders $T^{(N,u)}$ by Definition 7 is correct from the correctness of the generalized k-LC algorithm. Moreover it is obvious that p branches are needed at the generalized Lauder-Paterson algorithm from definition of the k-LC, the Lauder-Paterson algorithm and the generalized k-LC algorithm. Because the lower border and the upper border to keep that condition

```
   input: GLP(S, Σ, N, c, r, t)
M = N/p, S^(N) = S, Σ^(N) = Σ
T^(M,u) for u = 0 to p − 2 by (5)
if N > 1 then
   if r < T^(M,0) = t' then GLP(b^(M,0), Σ_1^(M), M, c + (p − 1)M, r, t')
   for w = 1 to p − 2
    if r' = T^(M,w−1) < T^(M,w) = t' then GLP(b^(M,w), Σ_{w+1}^(M), M, c + (p−w−1)M, r', t')
   if r' = T^(M,p−2) < t then GLP(b^(M,p−1), Σ_p^(M), M, c, r', t)
else    /* N = 1 */
   α_h = −s_0^(1)
   m = min{σ(ℓ, 0)|1 ≤ ℓ ≤ q, ℓ ≠ h}
   if m < σ(h, 0) then output(m, c + 1)
   if σ(h, 0) < t then output(σ(h, 0), c)
```

Fig. 4. Generalized Lauder-Paterson algorithm

as similar as the Lauder-Paterson algorithm, it is induced the correctness of proposed algorithm from the generalized k-LC algorithm and the Lauder-Paterson algorithm. □

Next we analyze memory and computation complexities about the generalized Lauder-Paterson algorithm.

Firstly we consider memory complexity in the single step of the algorithm. Four values M, c, r, t, each elements of $\Sigma^{(M)}$ and $p-1$ times $T^{(M,u)}$ are integers less than or equal to N, and the number of them is $p^m M + p + 3$. The elements of sequence $S^{(M)}$ has M elements over $GF(p^m)$. If we can use p-state memory, we need $n(p^m M + p + 3) + Mm$ memories from $N = p^n$ in the worst case of the single step. Because the algorithm runs from $M = p^{n-1}$ to 1 (n steps), we need $n^2(p+3) + p^n(np^m + m)$ memories in the worst case of the whole algorithm.

Secondly we consider computation complexity in the single step of the algorithm. Mp^{mp+1} times addition operations are needed for one $T^{(M,u)}$ calculation. Since u runs $p-1$ times, we need $(p-1)Mp^{mp+1}$ additions over $GF(p^m)$ from Definition 7. Moreover we need $p^m Mp^{mp+1} = Mp^{m(p+1)+1}$ additions for $\Sigma_w^{(M)}$ and Mp^2 times additions for $\boldsymbol{b}^{M,w}$. Consequently about $Mp^{m(p+1)+2}$ additions are needed in the single step of the algorithm. If we decide one extended decrease point, the algorithm runs from $M = p^{n-1}$ to $M = 1$ (n steps). Hence we need about $p^n p^{m(p+1)+2} = p^{n+m(p+1)+2}$ additions for one extended decrease point. Since the number of the extended decrease set is N in the worst case, the computation complexity of the algorithm is about $Np^{n+m(p+1)+2} = p^{2n+m(p+1)+2}$ additions.

6 Numerical Examples

In this section we consider balanced exponent periodic sequences [7] defined as follows.

Definition 10. *If an exponent periodic sequence S over $K = GF(p^m)$ has period p^n with $n \geq m$ and same distributions for all elements in K, i.e., the number of an*

element within one period is p^{n-m} for all elements in K, then a sequence S is called a balanced exponent periodic sequence (BEPS). □

Especially, if a binary exponent periodic sequence S is balanced sequence we call S a balanced binary exponent periodic sequence (BBEPS).

6.1 Binary Exponent Periodic Sequences with Period 16

In this section a numerical example of BEPS with period 16 using the LPA [9] is given in order to study about distributions on the profile of the k-LC. We show all profiles of them in Table.1, where # is the number of BBEPS with that profile except the periodic isomorphism, and selected lines in Fig.5. In except the periodic isomorphism [7], the number of all BBEPS is 800 and the number of BBEPS with condition of Seq.5 at Table.5 is 16.

Table 1. k-LC of BBEPS ($N = 16$)

k	0	2	4	6	#	k	0	2	4	6	#
Seq.1	15	10	5	2	128		14	3	3	3	8
	15	10	3	2	64	Seq.3	13	13	3	3	64
	15	9	9	2	128		13	13	2	2	32
	15	6	3	2	32	Seq.4	12	9	9	5	32
	15	5	5	2	32		12	7	2	2	8
	15	3	3	2	8		12	6	3	3	4
Seq.2	15	2	2	2	8		12	5	5	5	8
	14	11	5	3	64		11	11	5	5	16
	14	11	2	2	32		11	11	2	2	8
	14	9	9	3	64		10	10	5	5	8
	14	7	2	2	16		10	10	3	3	4
	14	5	5	3	16	Seq.5	9	9	9	9	16
									Total		800

6.2 Exponent Periodic Sequences over $GF(3)$ with Period 9

In order to study about distributions on the profile of the k-LC, we show numerical examples to apply the generalized Lauder-Paterson (LP) algorithm to a balanced exponent periodic sequence (BEPS) S over $GF(3)$ with period $9(= 3^2)$. Note that $[0\ 3\ 3]^t$ shows a matrix $\begin{bmatrix} 0 \\ 3 \\ 3 \end{bmatrix}$ in next example 1.

Example 1: [**Example of Generalized LP Algorithm**]

$$S^{(9)} = (220211010), \quad \Sigma^{(9)} = \begin{bmatrix} 000000000 \\ 111111111 \\ 111111111 \end{bmatrix}$$

[Depth 1]:

$$\boldsymbol{b}^{(3,0)} = (111), \quad \boldsymbol{b}^{(3,1)} = (021), \quad \boldsymbol{b}^{(3,2)} = (220),$$

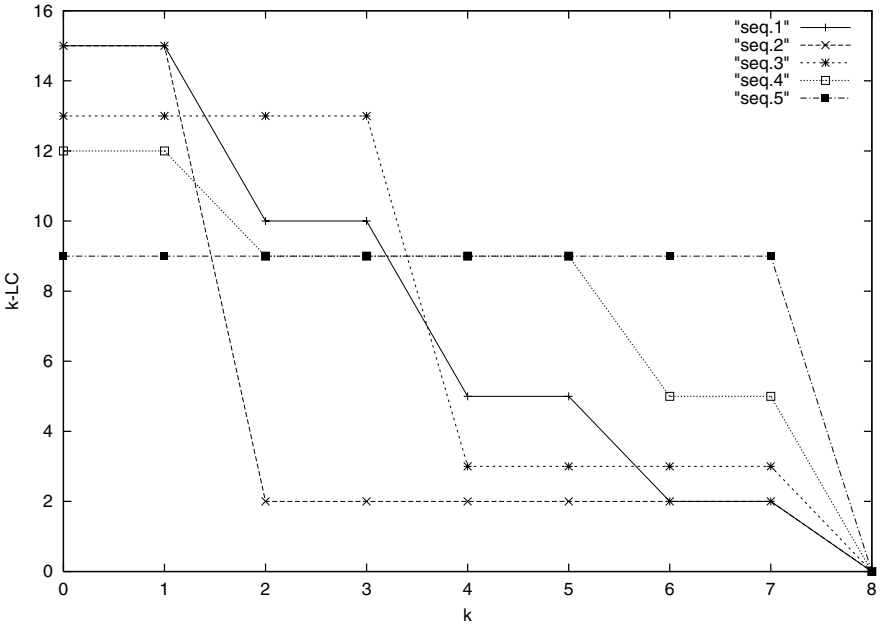

Fig. 5. Profile of k-LC for BBEPS ($N = 16$)

$$c = 0, \quad r = 0, \quad T^{(3,0)} = 3, \quad T^{(3,1)} = 3, \quad t = 10$$

$$\text{Case 1} : \texttt{GLP}(\boldsymbol{b}^{(3,0)} = (111), \begin{bmatrix} 000 \\ 111 \\ 111 \end{bmatrix}, 3, 6, 0, 3),$$

$$\text{Case 3} : \texttt{GLP}(\boldsymbol{b}^{(3,2)} = (220), \begin{bmatrix} 121 \\ 232 \\ 313 \end{bmatrix}, 3, 0, 3, 10)$$

[Depth 2]: of Case 1 at Depth 1

$$\boldsymbol{b}^{(1,0)} = (0), \quad \boldsymbol{b}^{(1,1)} = (0), \quad \boldsymbol{b}^{(1,2)} = (1),$$

$$c = 6, \quad r = 0, \quad T^{(1,0)} = 0, \quad T^{(1,1)} = 0, \quad t = 3$$

$$\text{Case 3} : \texttt{GLP}(\boldsymbol{b}^{(1,2)} = (1), [0\ 3\ 3]^t, 1, 6, 0, 3)$$

[Depth 2]: of Case 3 at depth 1

$$\boldsymbol{b}^{(1,0)} = (1), \quad \boldsymbol{b}^{(1,1)} = (0), \quad \boldsymbol{b}^{(1,2)} = (2),$$

$$c = 0, \quad r = 3, \quad T^{(1,0)} = 3, \quad T^{(1,1)} = 6, \quad t = 10$$

$$\text{Case 2} : \texttt{GLP}(\boldsymbol{b}^{(1,1)} = (0), [6\ 6\ 3]^t, 1, 1, 3, 6),$$

$$\text{Case 3} : \texttt{GLP}(\boldsymbol{b}^{(1,2)} = (2), [6\ 6\ 6]^t, 1, 0, 6, 10)$$

[Depth 3]: of Case 3 at Dep.2 and Case 1 at Dep.1

$$c = 6, \quad m = 0, \quad \sigma(3,0) = 3, \quad t = 3, \quad \underline{\texttt{output}(0,7)}$$

[Depth 3]: of Case 2 at Dep.2 and Case 3 at Dep.1

$$c = 1, \quad m = 3, \quad \sigma(1,0) = 6, \quad t = 6, \quad \underline{\texttt{output}(3,2)}$$

[Depth 3]: of Case 3 at Dep.2 and Case 3 at Dep.1

$$c = 0, \quad m = 6, \quad \sigma(2,0) = 6, \quad t = 10, \quad \underline{\texttt{output}(6,0)}$$

$EDS(S^{(9)}) = \{(0,7),(3,2),(6,0)\}$ □

Table 2. k-LC of BEPS over $GF(3)$ ($N = 9$)

k	0	1	2	3	4	5	6	#
Seq.1	8	8	4	4	2	2	0	972
Seq.2	8	8	2	2	2	2	0	162
Seq.3	7	7	7	2	2	2	0	342
Seq.4	6	6	4	4	4	4	0	162
Seq.5	4	4	4	4	4	4	0	54
						Total		1674

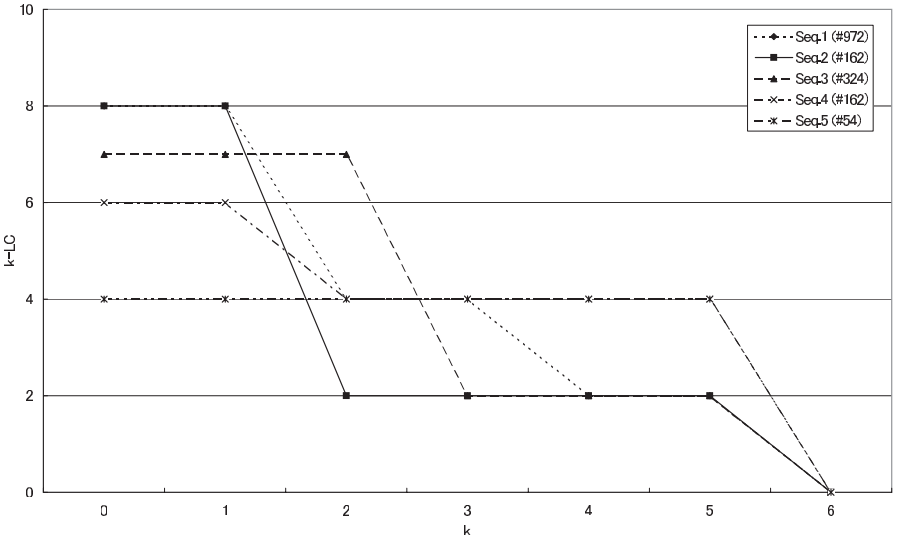

Fig. 6. Profile of k-LC for BEPS over $GF(3)$ ($N = 9$)

Example 2: [**Profiles of the k-LC for BEPS over $GF(3)$ with Period 9**]
A numerical example of BEPS over $GF(3)$ with $N = 9$ using the LPA [9]. We show all profiles of them in Table.2, where # is the number with that profile of BEPS's except the periodic isomorphism [13, 7], and all lines in Fig.6. □

7 Conclusion

In this paper we proposed the generalized Lauder-Paterson algorithm computing the profile of the k-LC for an exponent periodic sequence over a finite field. In order to derive proposed algorithm we recalled the generalized Games-Chan algorithm of the LC and the generalized k-LC algorithm for an exponent periodic sequence. The analysis of memory and computation complexities of the generalized Lauder-Paterson algorithm is given. Numerical examples of proposed algorithm for a BEPS over $GF(3)$ with period $9(= 3^2)$ is given to confirm the algorithm and all profiles and the number of them for BEPS over $GF(3)$ with period 9.

This proposed algorithm should be called a generalized k-LC spectrum [9] algorithm because this algorithm does not use the concepts of shift and offset. We may be able to rewrite proposed algorithm into an algorithm using the concepts of shift and offset.

Future works are fast algorithms of the LC and the k-LC for sequences with arbitrary period for fast algorithms for the k-LC. Moreover a generalization of the Lauder-Paterson algorithm using the concepts of shift and offset, remaining profiles of the k-LC for BEPS's and investigations of the k-LC and their profiles for non-binary sequences and non-exponent periodic sequences are also future works.

Acknowledgements

The author would like to thank Dr. Kenny Paterson for helpful discussion and bringing my attention to the paper [9] during the Second International Conference on Sequences and their Applications (SETA'01) in May, 2001 at Bergen, Norway. The author would like to thank Prof. Kyoki Imamura for encouragement and discussion to solve some problems on this area.

References

1. Z.Dai, and K.Imamura, "Linear Complexity for One-Symbol Substitution of a Periodic Sequence over $GF(q)$", *IEEE Trans. on Information Theory*, vol.44, pp.1328-1331, May, 1998.
2. C.Ding, G.Xiao, and W.Shan, *The Stability Theory of Stream Ciphers*, Lecture Notes in Computer Science, vol.561, Springer-Verlag, 1991.
3. R.Games, and A.Chan, "A Fast Algorithm for Determining the Complexity of a Binary Sequence with Period 2^n", *IEEE Trans. on Information Theory*, vol.IT-29, pp.144-146, Jan., 1983.
4. T.Kaida, S.Uehara, and K.Imamura, "An Algorithm for the k-Error Linear Complexity of Sequences over $GF(p^m)$ with Period p^n, p a Prime", *Information and Computation*, Vol.151, pp.134-147, Academic Press, May, 1999.
5. T.Kaida, S.Uehara, and K.Imamura, "A New Algorithm for the k-Error Linear Complexity of Sequences over $GF(p^m)$ with Period p^n", *Sequences and their Applications - Proceedings of SETA'98*, pp.284-296, Springer-Verlag, 1999.
6. T.Kaida, S.Uehara, and K.Imamura, "On the Profile of the k-Error Linear Complexity and the Zero Sum Property for Sequences over $GF(p^m)$ with Period p^n", *Sequences and their Applications - Proceedings of SETA'01*, pp.218-227, Springer-Verlag, 2001.

7. T.Kaida, "A Typical Profile of the k-Error Linear Complexity for Balanced Binary Sequences with Period 2^n", submitted to *IEICE Trans. Fundamentals*, Special Section of Cryptography and Information Security, Jan., 2005.
8. K.Kurosawa, F.Sato, T.Sakata, and W.Kishinoto, "A Relationship between Linear Complexity and k-Error Linear Complexity", *IEEE Trans. on Information Theory*, vol.46, pp.694-698, Mar., 2000.
9. A.G.B.Lauder, K.G.Paterson, "Computing the Error Linear Complexity Spectrum of a Binary Sequence of Period 2^n", *IEEE Trans. Inf. Theory*, vol.49, pp.273-280, Jan., 2003.
10. M.Stamp, and C.Martin, "An Algorithm for the k-Error Linear Complexity of Binary Sequences with Period 2^n", *IEEE Trans. on Information Theory*, vol.39, pp.1398-1401, July, 1993.
11. S.Uehara, and K.Imamura, "Linear Complexity of Periodic Sequences Obtained from $GF(q)$ Sequences with Period $q^n - 1$ by One-Symbol Insertion", *IEICE Trans. on Fundamentals*, vol.E79-A, pp.1739-1740, Oct., 1996.
12. S.Uehara, and K.Imamura, "Linear Complexity of Periodic Sequences Obtained from $GF(p)$ Sequences with Period $p^n - 1$ by One-Symbol Deletion", *IEICE Trans. on Fundamentals*, vol.E80-A, pp.1164-1166, June, 1997.
13. S.Uehara, K.Imamura, T.Kaida, "Value distribution of linear complexity for q-ary periodic sequences with period p^n, p a prime", *IEICE Trans. Fundamentals*, vol.E80-A, pp.920-921, May, 1997.