Trace Representation of Lempel-Cohn-Eastman Sequences

Sang-Hyo Kim, Jong-Seon No
School of Electrical Engineering
Seoul National University

and Tor Helleseth
Department of Informatics
University of Bergen

ABSTRACT

Lempel, Cohn and Eastman introduced a sequence (LCE sequence) of even period with the optimal autocorrelation property in 1977. But its linear complexity and trace representation have been unknown. Recently, the linear complexity of LCE sequences was computed[1]. In this paper, the trace representations for LCE sequences of period $p^m - 1$ for $p = 3$ and 5 are derived by computing the values of all Fourier coefficients in F_p for the sequences.

1. Introduction

Among properties of periodic sequences, the linear complexity [6], balance and correlation properties are important for the application of stream ciphers and CDMA communication systems. A binary sequence is said to have the balance property if the difference between the number of 1's and 0's in a period of the sequence is at most one. Let $s(t)$ be a binary sequence of period n. The autocorrelation function of a binary sequences of period n is defined as

$$R(\tau) = \sum_{t=0}^{n-1} (-1)^{s(t)+s(t+\tau)}.$$

A sequence is defined to have the ideal autocorrelation if

$$R(\tau) = \begin{cases} n, & \text{if } \tau = 0 \mod n \\ -1, & \text{otherwise.} \end{cases}$$

Then a binary sequence of even period n with the balance property is said to have optimal autocorrelation if

$$R(\tau) = \begin{cases} 0 \text{ or } -4, & \text{if } n = 0 \mod 4 \\ 2 \text{ or } -2, & \text{if } n = 2 \mod 4. \end{cases}$$

Let p be an odd prime and m an integer. Let F_{p^m} be a finite field with p^m elements and $F_{p^m}^* = F_{p^m} \backslash \{0\}$. Let S be a nonempty subset of $F_{p^m}^*$ and α be a primitive element of F_{p^m}. Then the characteristic sequence of period $p^m - 1$ of the set S is defined as [7]

$$s(t) = \begin{cases} 1, & \text{if } \alpha^t \in S \\ 0, & \text{otherwise.} \end{cases} \quad (1)$$

Let S be a set defined as[3][7]

$$S = \{\alpha^{2i+1} - 1 \mid 0 \le i \le \frac{p^m - 1}{2} - 1\},$$

where α is a primitive element of F_{p^m}. Then the characteristic sequence of the set S defined in (1) is referred to as a *Lempel-Cohn-Eastman (LCE) sequence* [2][3], which is a 0-1 binary sequence of period $p^m - 1$, *i.e.*, of even length with the optimal autocorrelation property. No, Chung, Song, Yang, Lee and Helleseth also introduced sequences by using the image of the polynomial $(z+1)^d + az^d + b$ over F_{p^m} [4], which turned out to be LCE sequences.

Helleseth and Yang expressed the LCE sequences by using the indicator function and the quadratic character given by [7]

$$s(t) = \frac{1}{2}(1 - I(\alpha^t + 1) - \chi(\alpha^t + 1)), \quad (2)$$

where the indicator function $I(x) = 1$ if $x = 0$ and $I(x) = 0$ otherwise and $\chi(x)$ denotes the quadratic character of x. Helleseth and Yang also worked on the linear complexity over F_2, of LCE sequences [7]. But it is more natural to find the linear complexity over F_p because it is constructed on F_{p^n}. Recently, the linear complexity over F_p was computed by Helleseth, Kim and No[1].

The trace representation of sequences is useful for implementing the generator of sequences and analyzing their properties [5][6]. Thus it is of great interests to represent the LCE sequences by using the trace functions.

In this paper, the trace representations for LCE sequences of period $p^m - 1$ for $p = 3$ and 5 are found by computing the values of all Fourier coefficients in F_p for the sequences.

2. Trace Representation of LCE Sequences of Period $p^n - 1$

In this section, the trace representation of LCE se-

quences of period $p^m - 1$ for $p = 3$ and 5 is derived by using the trace functions from F_{p^k} to F_p, where $k|m$, even though they are binary sequences.

It is well known that using the Fourier transform of a p-ary sequence $s(t)$ of period $n = p^m - 1$ in the finite field F_{p^n} is given as

$$A_i = \frac{1}{n} \sum_{t=0}^{n-1} s(t)\alpha^{-it} \tag{3}$$

and its inverse Fourier transform as

$$s(t) = \sum_{i=0}^{n-1} A_i \alpha^{it}, \tag{4}$$

where α is a primitive element of F_{p^m} and $A_i \in F_{p^m}$.

Using the Fourier transform of the sequences, we first find an expression for A_{-i}, $0 \le i \le n-1$ of LCE sequences as in the following lemma which is important to achieve the goal of this section.

Lemma 1 [Helleseth, Kim and No [1]]: A_{-i} of the LCE sequences defined in (2) is given as

$$(p-2)A_{-i} = -(-1)^i + (-1)^{i-\frac{p^m-1}{2}} \cdot \prod_{a=0}^{m-1} \binom{i_a}{\frac{p-1}{2}} \mod p. \tag{5}$$

□

Let $(i_0, i_1, i_2, \cdots, i_{m-1})$ be a vector corresponding to the coefficients in the p-adic expansion $\sum_{a=0}^{m-1} i_a p^a$ of $i, 0 \le i \le p^m - 2$. It is clear that all integers corresponding to the cyclic shift of vector $(i_0, i_1, i_2, \cdots, i_{m-1})$ belong to the same cyclotomic coset of F_{p^m}. Thus it is obvious that all A_i's in a coset have the same value from (5). Therefore, the equation (4) can be expressed as a linear combination of the trace functions over F_p given by

$$s(t) = \sum_{a \in L} A_a \cdot tr_1^k(\alpha^{at}), \tag{6}$$

where L is a set of coset leaders of F_{p^m} and a is a coset leader that F_{p^k} is a smallest subfield of F_{p^m} such that $\alpha^a \in F_{p^k}$.

The trace representation of the sequences of period $p^m - 1$ is derived by computing all coefficients A_i's, $0 \le i \le p^m - 2$ in (5) for the LCE sequences in (2).

A. Trace Representation over F_3 of LCE Sequences of Period $3^m - 1$

In order to find the trace representation of LCE sequences of period $3^m - 1$, we will define the trace functions as follows. Let $tr(\alpha^{at})$ be a trace function from F_{3^k} to F_3, where $k|m$ and F_{3^k} is a smallest subfield of F_{3^m} such that $\alpha^a \in F_{3^k}$. That is, for F_{3^4}, $tr(\alpha^{0t}) = tr_1^1(\alpha^{0t}) = tr_1^1(1) = 1$, because $\alpha^0 \in F_3$. $tr(\alpha^{40t}) = tr_1^1(\alpha^{40t}) = tr_1^1((-1)^t) = (-1)^t$, because $\alpha^{40} \in F_3$. $tr(\alpha^{20t}) = tr_1^2(\alpha^{20t})$, because $\alpha^{20} \in F_{3^2}$.

We can classify the coset leaders of the finite field $F_{3^m}^*$ as follows:

I_1^o : Set of odd coset leaders, where every digit in the 3-adic expansion of coset leader only takes the values '1' or '0'. (ex) $13 = 1 + 3 + 9 = (1, 1, 1)$

I_1^e : Set of even coset leaders excluding coset leader 0, where every digit only takes the values '1' or '0'. (ex) $10 = 1 + 9 = (1, 0, 1)$

I^o : Set of odd coset leaders including I_1^o.

I^e : Set of even coset leaders including I_1^e.

Using the above notation, the trace representation of LCE sequence of period $3^m - 1$ is given in the following theorem.

Theorem 2 : The trace representation of LCE sequence of period $n = 3^m - 1$ is given by

$$s(t) = \sum_{a_i \in I^o \setminus I_1^o} tr(\alpha^{a_i t}) + 2 \cdot \sum_{a_i \in I^e \setminus I_1^e} tr(\alpha^{a_i t}) + 2 \cdot \sum_{a_i \in I_1^o} tr(\alpha^{a_i t}),$$

where α is a primitive element of finite field F_{3^m} and $tr(\alpha^{at})$ is a trace function from F_{3^k} to F_3 for $k|m$ and F_{3^k} is a smallest subfield of F_{3^m} such that $\alpha^a \in F_{3^k}$.

Proof: For LCE sequences of period $3^m - 1$, the coefficients $A_i \in F_3$, $0 \le i \le 3^m - 2$ defined in (5) can be rewritten as

$$A_{-i} = -(-1)^i + (-1)^{i-\frac{3^m-1}{2}} \prod_{a=0}^{m-1} \binom{i_a}{1} \mod 3. \tag{7}$$

Now, we have to find all A_i's, $0 \le i \le 3^m - 2$ for the trace representation of LCE sequences of period $3^m - 1$. For $i = 0$, it is easy to find that $A_0 = 2$. Clearly, for odd m, $\frac{3^m-1}{2} = 1 \mod 2$ and for even m, $\frac{3^m-1}{2} = 0 \mod 2$. Then the equation (7) can be modified as follows:

$$\prod_{a=0}^{m-1} \binom{i_a}{1} = \prod_{a=0}^{m-1} i_a = (A_{-i} + (-1)^i)(-1)^{m-i} \mod 3. \tag{8}$$

Note that $j = -i = n - i$, $1 \le j \le 3^m - 2$, where A_0 for $j = i = 0$ is already found. In the 3-adic expansion of $i = \sum_a i_a 3^a$ and $j = \sum_a j_a 3^a$, it is clear that $j_a = p - 1 - i_a = 2 - i_a$ for all a, $0 \le a \le m-1$.

Let us consider three cases as follows:

Case 1: $A_{-i} = A_j = 0$:

We have to find all $j = n - i$, $1 \le j \le 3^m - 2$ such that $A_{-i} = 0$ in (8), which is rewritten as

$$\prod_a i_a = (-1)^m \mod 3. \tag{9}$$

Necessary condition for the equation (9) is that i_a's in the 3-adic expansion $\sum_a i_a 3^a$ of i only take the values '1' or '2', which means that j_a's only take the values

'0' or '1'. Since $2 = -1 \mod 3$ and $2^2 = 1 \mod 3$, the number of occurrences $i_a = 2$, $0 \le a \le m-1$ in the 3-adic expansion of i satisfying (9) should be odd for odd m and even for even m and thus the number of occurrences $i_a = 1$ should be even for any integer m. Therefore, the number of '1' in the list of $j_a, 0 \le a \le m-1$ should be even for any integer m and thus j is even. Thus, the coset leader of j such that $A_j = 0$ belongs to the set I_1^e, where $j = 0$ is excluded.

Case 2: $A_{-i} = A_j = 1$:

In this case, we have to find all $j = n - i, 1 \le j \le 3^m - 2$ such that $A_j = 1$ in (8). The following two subcases are considered:

(i) Case of i = even integer (*i.e.*, j = even integer) :

We can rewrite the equation (8) as

$$\prod_a i_a = -(-1)^m \mod 3, \tag{10}$$

where all i_a's have to take the values '1' or '2'. The number of $i_a = 2$ should be odd for even m and even for odd m, which means that the number of $i_a = 1$, $0 \le a \le m-1$ should be odd for any integer m. Therefore, all j_a's only take the value '0' or '1' and the number of $j_a = 1$ should be odd for any integer m, which means that j is odd. It contradicts to the assumption that j is an even integer. Therefore, there is no even integer j which makes $A_j = 1$.

(ii) Case of i = odd integer (*i.e.*, j = odd integer):

The equation (8) can be written as:

$$\prod_a i_a = 0 \mod 3. \tag{11}$$

The equation (11) means that at least one of i_a's has to take the value '0', which means that at least one of j_a's has to take the value '2'. Therefore, the coset leader of j belongs to the set $I^o \backslash I_1^o$.

Case 3: $A_{-i} = A_j = 2$:

In this case, all $j = n - i$, $1 \le j \le 3^m - 2$ such that $A_j = 2$ in (8), have to be determined, which can be easily found because we already found all j's such that $A_j = 0$ or 1. Clearly, the remaining sets of coset leaders in $F_{3^m}^*$ are $I^e \backslash I_1^e$ and I_1^o. □

B. Trace Representation over F_5 of LCE Sequences of Period $5^m - 1$

For the period $5^m - 1$, the trace representation of LCE sequences is derived similar to the case of period $3^m - 1$. Let $tr(\alpha^{at})$ be a trace function from F_{5^k} to F_5, where $k|m$ and F_{5^k} is a smallest subfield of F_{5^m} such that $\alpha^a \in F_{5^k}$.

The coset leaders of the finite field $F_{5^m}^*$ can be classified as follows:

I_1^o : Set of odd coset leaders, where every digit in the 5-adic expansion of coset leader only takes the values '0', '1' or '2' and the number of '1' is 1 mod 4.

I_3^o : Set of odd coset leaders, where every digit only takes the values '0', '1' or '2' and the number of '1' is 3 mod 4.

I_0^e : Set of even coset leaders excluding coset leader 0, where every digit only takes the values '0', '1' or '2' and the number of '1' is 0 mod 4.

I_2^e : Set of even coset leaders, where every digit only takes the values '0', '1' or '2' and the number of '1' is 2 mod 4.

I^o : Set of odd coset leaders including I_1^o and I_3^o.

I^e : Set of even coset leaders including I_0^e and I_2^o.

Using the above notation, the trace representation of LCE sequence of period $5^m - 1$ is given in the following theorem.

Theorem 3 : The trace representation of LCE sequence of period $n = 5^m - 1$ is given by

$$\begin{aligned} s(t) \;=\; & \sum_{a_i \in I^o \backslash \{I_1^o \cup I_3^o\}} 2 \cdot tr(\alpha^{a_i t}) + \sum_{a_i \in I^e \backslash \{I_0^e \cup I_2^e\}} 3 \cdot tr(\alpha^{a_i t}) \\ & + \sum_{a_i \in I_1^o} tr(\alpha^{a_i t}) + \sum_{a_i \in I_3^o} 3 \cdot tr(\alpha^{a_i t}) + \sum_{a_i \in I_2^e} tr(\alpha^{a_i t}), \end{aligned}$$

where α is a primitive element of finite field F_{5^m} and $tr(\alpha^{at})$ is a trace function from F_{5^k} to F_5 for $k|m$ and F_{5^k} is a smallest subfield of F_{5^m} such that $\alpha^a \in F_{5^k}$.

Proof: Because the proof of this theorem is very similar to the proof of the case $p = 3$, we somewhat brief it. For LCE sequences of period $5^m - 1$, the coefficients $A_i \in F_5$, $0 \le i \le 5^m - 2$ defined in (5) can be rewritten as

$$3A_{-i} = -(-1)^i + (-1)^{i - \frac{5^m - 1}{2}} \prod_{a=0}^{m-1} \binom{i_a}{2} \mod 5. \tag{12}$$

Now, we have to find all A_i's, $0 \le i \le 5^m - 2$.

For $i = 0$, it is easy to find $A_0 = 3$ from the equation (12). Using $\frac{5^m - 1}{2}$ = even, the equation (12) can be rewritten as

$$\prod_{a=0}^{m-1} \binom{i_a}{2} = (3 \cdot A_{-i} + (-1)^i) \cdot (-1)^{-i} \mod 5. \tag{13}$$

As 3 is a generator of F_5, we have $3^0 = 1, 3^1 = 3, 3^2 = 4, 3^3 = 2, 3^4 = 1$. Note that $j = -i = n - i$, $1 \le j \le 5^m - 2$. In the 5-adic expansion of $i = \sum_a i_a 5^a$ and $j = \sum_a j_a 5^a$, it is clear that $j_a = 4 - i_a$ for all a, $0 \le a \le m-1$.

Let us consider the following five cases:

Case 1: $A_{-i} = A_j = 0$:

We have to find all $j = n-i$, $1 \le j \le 5^m - 2$ such that $A_{-i} = 0$. Let i be an integer such that $A_{-i} = A_j = 0$. Then (13) can be written as $\prod_{a=0}^{m-1} \binom{i_a}{2} = 1 \mod 5$. Since $\binom{i_a}{2}$ is equal to zero for $0 \le i_a \le 1$, j_a's satisfy the following relation:

> number of occurrences $j_a = 1$ in the 5-adic expansion of j is $0 \mod 4$.

Thus j is an even integer. Therefore, the coset leader of j such that $A_j = 0$ belongs to the set I_0^e.

Case 2: $A_{-i} = A_j = 1$:

Here all $j = n - i$, $1 \le j \le 5^m - 2$ satisfying $A_{-i} = 1$ are determined. Let i be an integer such that $A_{-i} = A_j = 1$. Then we have to consider the following two subcases:

(i) Case of i = even integer (*i.e.*, j = even integer):

Then (13) can be expressed as $\prod_{a=0}^{m-1} \binom{i_a}{2} = 4 \mod 5$. To satisfy the above equation, j_a's have to satisfy:

> number of occurrences $j_a = 1$ in the 5-adic expansion of j is $2 \mod 4$.

The integer j is even. Thus the coset leader of j such that $A_j = 1$ belongs to the set I_2^e.

(ii) Case of i = odd integer (*i.e.*, j = odd integer):

The equation (13) becomes $\prod_{a=0}^{m-1} \binom{i_a}{2} = 3 \mod 5$. To satisfy the condition, j_a's have to satisfy:

> number of occurrences $j_a = 1$ in the 5-adic expansion of j is $1 \mod 4$.

Thus j is an odd integer. Thus the coset leader of j such that $A_j = 1$ belongs to the set I_1^o.

Case 3: $A_{-i} = A_j = 2$:

We determine all $j = n-i$, $1 \le j \le 5^m - 2$ such that $A_{-i} = 2$. Let i be an integer such that $A_{-i} = A_j = 2$. Then the following two subcases are considered:

(i) Case of i = even integer (*i.e.*, j = even integer):

We can rewrite the equation (13) as $\prod_{a=0}^{m-1} \binom{i_a}{2} = 2 \mod 5$. To satisfy the equation, j_a's must satisfy:

> number of occurrences $j_a = 1$ in the 5-adic expansion of j is $3 \mod 4$.

Thus j is an odd integer, which contradicts to the assumption that j is an even integer.

(ii) Case of i = odd integer (*i.e.*, j = odd integer):

In this case the equation (13) can be expressed as $\prod_{a=0}^{m-1} \binom{i_a}{2} = 0 \mod 5$. To satisfy the condition, at least one of j_a's has to take the values '3' or '4'. Thus the coset leader of j such that $A_j = 2$ belongs to the set $I^o \backslash \{I_1^o \bigcup I_3^o\}$.

Case 4: $A_{-i} = A_j = 3$:

We have to find all $j = n-i$, $1 \le j \le 5^m - 2$ such that $A_{-i} = 3$. Let i be an integer such that $A_{-i} = A_j = 3$. Then we have to consider the following two subcases:

(i) Case of i = even integer (*i.e.*, j = even integer):

Then the equation (13) can be modified as $\prod_{a=0}^{m-1} \binom{i_a}{2} = 0 \mod 5$. To satisfy the equation, the coset leader of j such that $A_j = 3$ belongs to the set $I^e \backslash \{I_0^e \bigcup I_2^e\}$, where coset leader 0 is included.

(ii) Case of i = odd integer (*i.e.*, j = odd integer):

Then the equation (13) can be expressed as $\prod_{a=0}^{m-1} \binom{i_a}{2} = 2 \mod 5$. To satisfy the above equation, j must belong to the set I_3^o.

Case 5: $A_{-i} = A_j = 4$:

There is no coset leader i which satisfies $A_{-i} = A_j = 4$ since all coset leaders were considered in the former cases. □

References

[1] T. Helleseth, S.H. Kim, J.S. No, "Linear complexity over F_p of LCE sequences," *Proceedings of 2nd CITW 2001*, Seoul Korea, October 13, 2001.

[2] V.M. Sidelnikov, "Some k-valued pseudo-random and nearly equidistant codes," *Problemy Peredachi Informatsii*, vol. 5, No. 1, pp. 16-22, 1969.

[3] A. Lempel, M. Cohn and W.L. Eastman, "A class of binary sequences with optimal autocorrelation properties," *IEEE Trans. Inform. Theory*, vol. 23, No. 1, pp. 38-42, Jan. 1977.

[4] J.S. No, H. Chung, H.Y. Song, K. Yang, J.D. Lee and T. Helleseth, "New construction for binary sequences of period $p^m - 1$ with optimal autocorrelation using $(z+1)^d + az^d + b$," *IEEE Trans. Inform. Theory*, vol. 47, No. 4, pp. 1638-1644, May 2001.

[5] J.S. No, H.K. Lee, H. Chung, H.Y. Song and K. Yang, " Trace representation of Legendre sequence of Mersenne prime period," *IEEE Trans. Inform. Theory*, vol. 42, no.3, pp. 2254-2255, Nov. 1996.

[6] C. Ding, T. Helleseth and W. Shan, "On the linear complexity of Legendre sequences," *IEEE Trans. Inform. Theory*, vol. 44, no.3, pp. 1276-1278, May 1998.

[7] T. Helleseth and K. Yang, "On binary sequences of period $n = p^m - 1$ with optimal autocorrelation," *Proceedings of 2001 Sequences and Their Applications* (SETA '01), pp. 29-30, Bergen, Norway, May 13-17, 2001.