# Linear Complexity Over $F_p$ and Trace Representation of Lempel–Cohn–Eastman Sequences

Tor Helleseth, *Fellow, IEEE*, Sang-Hyo Kim, *Student Member, IEEE*, and Jong-Seon No, *Member, IEEE*

***Abstract*—In this correspondence, the linear complexity over $F_p$ of Lempel–Cohn–Eastman (LCE) sequences of period $p^m - 1$ for an odd prime $p$ is determined. For $p = 3, 5$, and $7$, the exact closed-form expressions for the linear complexity over $F_p$ of LCE sequences of period $p^m - 1$ are derived. Further, 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.**

***Index Terms*—Lempel–Cohn–Eastman (LCE) sequences, linear complexity, sequences.**

## I. Introduction

Among properties of periodic sequences [1], [8], the linear complexity [5], [6], [20], [24], balance, and correlation properties are important for the application of stream ciphers and code-division multiple-access (CDMA) communication systems [22]. 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 sequence 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 ideal autocorrelation if

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

A lot of attention [7], [8], [17], [19] has been devoted to binary sequences of period $2^m - 1$ with ideal autocorrelation. A binary sequence of even period $n$ with the balance property is said to have optimal autocorrelation if

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

Let $p$ be a prime and $m$ be a positive integer. Let $F_{p^m}$ be the 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 $\alpha$ a primitive element of $F_{p^m}$. Then the characteristic sequence of period $p^m - 1$ of the set $S$ is defined as [9]

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

Let $S$ be a set defined as [9], [12]

$$S = \left\{ \alpha^{2i+1} - 1 \,\middle|\, 0 \le i \le \frac{p^m - 1}{2} - 1 \right\}$$

where $p$ is an odd prime and $\alpha$ is a primitive element of $F_{p^m}$. Then, the characteristic sequence of this set $S$ is referred to as a *Lempel–Cohn–Eastman (LCE) sequence* [12], [21], which is a $0$-$1$ binary sequence of period $p^m - 1$, i.e., of even length. It has been shown that LCE sequences have the optimal autocorrelation and balance property. No *et al.*[15] also introduced binary sequences of period $p^m - 1$ with optimal autocorrelation property by using the image of the polynomial $(z+1)^d + az^d + b$ over $F_{p^m}$, which turned out to be LCE sequences.

Let $\chi(x)$ denote the quadratic character of $x$ defined by

$$\chi(x) = \begin{cases} +1, & \text{if } x \text{ is a quadratic residue} \\ 0, & \text{if } x = 0 \\ -1, & \text{if } x \text{ is a quadratic nonresidue.} \end{cases} \tag{2}$$

Helleseth and Yang [9] described LCE sequences by using the indicator function and the quadratic character given by

$$s(t) = \frac{1}{2}\left(1 - I(\alpha^t + 1) - \chi(\alpha^t + 1)\right) \tag{3}$$

where the indicator function $I(x) = 1$ if $x = 0$ and $I(x) = 0$ otherwise.

Helleseth and Yang [9] studied the linear complexity over $F_2$ of LCE sequences. Even though LCE sequences are binary sequences, they are constructed based on the finite field $F_{p^m}$ and, thus, it is more natural to find the linear complexity over $F_p$ for LCE sequences. The trace representation of sequences is useful for implementing the generator of sequences and analyzing their properties [6], [11], [18]. Thus, it is of great interest to represent LCE sequences by using the trace functions.

In this correspondence, the linear complexity over $F_p$ of LCE sequences of period $p^m - 1$ for an odd prime $p$ is determined. For $p = 3, 5$, and $7$, the exact closed-form expressions for the linear complexity over $F_p$ of LCE sequences of period $p^m - 1$ are derived. Further, 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.

## II. Linear Complexity Over $F_p$ of LCE Sequences of Period $p^m - 1$

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

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

and its inverse Fourier transform as

$$s(t) = \sum_{i=0}^{n-1} A_i \alpha^{it} \tag{5}$$

where $\alpha$ 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.

*Lemma 1:* Let the $p$-adic expansion of $i$ be given as

$$i = \sum_{a=0}^{m-1} i_a p^a \tag{6}$$

where $0 \le i_a \le p - 1$. Then, $A_{-i}$ of the LCE sequences defined in (3) is given as

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

Manuscript received August 14, 2001; revised January 22, 2003. This work was supported in part by BK21, ITRC, and The Norwegian Research Council.

T. Helleseth is with the Department of Informatics, University of Bergen, N-5020 Bergen, Norway (e-mail: Tor.Helleseth@ii.uib.no).

S.-H. Kim and J.-S. No are with the School of Electrical Engineering and Computer Science, Seoul National University, Seoul, Korea (e-mail: kimsh@ccl.snu.ac.kr; jsno@snu.ac.kr).

Communicated by A. M. Klapper, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2003.811924

*Proof:* Using the Fourier transform of the sequences in (4), the relation for $A_{-i}$ can be derived as follows:

$$\begin{aligned}2nA_{-i} &= 2\sum_{t=0}^{n-1} s(t)\alpha^{it}\\ &= \sum_{t=0}^{n-1}(1 - I(\alpha^t+1) - \chi(\alpha^t+1))\alpha^{it}\\ &= \sum_{t=0}^{n-1}\alpha^{it} - (-1)^i - \sum_{t=0}^{n-1}\chi(\alpha^t+1)\alpha^{it}. \end{aligned} \tag{8}$$

For $i=0$, (8) can be given as

$$\begin{aligned}2nA_0 &= p^m - 1 - 1 - \sum_{t=0}^{n}\chi(\alpha^t+1)\\ &= p^m - 2 - \left[\left\{\sum_{t=0}^{n}\chi(\alpha^t+1)+\chi(1)\right\} - \chi(1)\right]\\ &= p^m - 2 - 0 + 1\\ &= -1 \bmod p.\end{aligned}$$

Thus, we have proved that the lemma holds for $i=0$.

For nonzero $i$, (8) can be rewritten as

$$\begin{aligned}2nA_{-i} &= -(-1)^i - \sum_{x\in F_{p^m}^*}\chi(x+1)x^i\\ &= -(-1)^i - \sum_{y\in F_{p^m}}\chi(y)(y-1)^i.\end{aligned} \tag{9}$$

As $z$ varies over $F_{p^m}$, $z^2$ takes all the quadratic residues in $F_{p^m}$ exactly twice and the zero element once. Similarly, $\alpha z^2$ takes all the quadratic nonresidues in $F_{p^m}$ as values exactly twice and the zero element once. It is clear that all the quadratic residues and nonresidues together with the element 0 cover all elements in $F_{p^m}$.

Using the definition of the quadratic character $\chi(\cdot)$ in (2), (9) is modified as

$$\begin{aligned}2nA_{-i} &= -(-1)^i\\ &\quad - \frac{1}{2}\sum_{z\in F_{p^m}}[\chi(z^2)(z^2-1)^i + \chi(\alpha z^2)(\alpha z^2-1)^i]\\ &= -(-1)^i - \frac{1}{2}\sum_{z\in F_{p^m}}[(z^2-1)^i - (\alpha z^2-1)^i]\\ &= -(-1)^i - \frac{1}{2}\sum_{l=0}^{i}\binom{i}{l}(-1)^{i-l}(1-\alpha^l)\sum_{z\in F_{p^m}} z^{2l}.\end{aligned}$$

The inner sum only contributes when $l = \frac{p^m-1}{2}$, in this case $\alpha^l = -1$. Note that when $l=0$ then $1-\alpha^l = 0$. Therefore, we obtain

$$2nA_{-i} = -(-1)^i - (p^m-1)\binom{i}{\frac{p^m-1}{2}}(-1)^{i-\frac{p^m-1}{2}}.$$

Reducing modulo $p$ for both sides, we have the relation

$$(p-2)A_{-i} = -(-1)^i + \binom{i}{\frac{p^m-1}{2}}(-1)^{i-\frac{p^m-1}{2}} \bmod p. \tag{10}$$

From the result of Lucas [2] given by

$$\binom{i}{\frac{p^m-1}{2}} = \prod_{a=0}^{m-1}\binom{i_a}{\frac{p-1}{2}} \bmod p$$

(10) reduces to (7). □

It is already known from Blahut's theorem [3], [4] that the linear complexity of periodic sequences can be determined by computing the Hamming weight of their Fourier transform. Thus, we need to determine the cardinality of the set $\{i \mid A_{-i} \neq 0,\ 0 \le i \le n-1\}$, which is calculated from (7). We have proved the following result.

*Theorem 2:* Let $C$ be the number of integers $i$, $0 \le i \le p^m - 2$ satisfying the relation

$$\prod_{a=0}^{m-1}\binom{i_a}{\frac{p-1}{2}} = (-1)^{\frac{p^m-1}{2}} \bmod p \tag{11}$$

where the $i_a$'s are coefficients in the $p$-adic expansion $\sum_a i_a p^a$ of $i$. Then the linear complexity over $F_p$ of the LCE sequence of period $n = p^m - 1$ defined in (3) equals

$$L_p = n - C. \tag{12}$$

To demonstrate this technique, we will calculate the linear complexity over $F_p$ of the LCE sequence of period $n = p^m - 1$ in the case of $p = 3,\ 5$, and 7. But it is not easy to find the linear complexity over $F_p$ of LCE sequences for $p > 7$.

### A. Linear Complexity Over $F_3$ of LCE Sequences of Period $3^m - 1$

Using the result of Theorem 2, the linear complexity over $F_3$ of LCE sequences of period $n = 3^m - 1$ is derived in the following theorem.

*Theorem 3:* The linear complexity over $F_3$ of the LCE sequence of period $n = 3^m - 1$ is given as

$$L_3 = 3^m - 2^{m-1}.$$

*Proof:* For $p = 3$, it is clear that

$$\binom{0}{1} = 0, \quad \binom{1}{1} = 1, \quad \binom{2}{1} = 2$$

and

$$\frac{3^m-1}{2} = \begin{cases}\text{even}, & \text{if } m = \text{even}\\ \text{odd}, & \text{if } m = \text{odd}.\end{cases}$$

Then (11) is rewritten as

$$\prod_{a=0}^{m-1} i_a = (-1)^m \bmod 3. \tag{13}$$

Thus, all the $i_a$'s in the 3-adic expansion of $i$ should be 1 or 2. The number of solutions of this system is $2^{m-1}$ since selecting $i_0, i_1, \ldots, i_{m-2}$ uniquely determines $i_{m-1}$. However, even though it satisfies (13), the solution corresponding to

$$i_0 = i_1 = \cdots = i_{m-2} = 2$$

must be excluded since it corresponds to $i = 3^m - 1$. We conclude that $C = 2^{m-1} - 1$ and the linear complexity over $F_3$ of the LCE sequence of period $3^m - 1$ equals

$$L_3 = 3^m - 2^{m-1}.$$

□

### B. Linear Complexity Over $F_5$ of LCE Sequences of Period $5^m - 1$

In this case, the linear complexity over $F_5$ of LCE sequences of period $5^m - 1$ is derived by counting nonzero Fourier coefficients of the sequences as in the following theorem.

*Theorem 4:* The linear complexity over $F_5$ of the LCE sequence of period $n = 5^m - 1$ is given as

$$L_5 = 5^m - \sum_{j=0}^{\lfloor \frac{m}{4}\rfloor}\binom{m}{4j}\cdot 2^{m-4j}$$

where $\lfloor d \rfloor$ is the largest integer less than or equal to $d$.

*Proof:* Since $\frac{5^m-1}{2}$ is an even integer for any integer $m$, (11) for $p=5$ can be rewritten as

$$\prod_{a=0}^{m-1}\binom{i_a}{2}=1 \mod 5 \tag{14}$$

where the $i_a$'s are coefficients in the 5-adic expansion $\sum_a i_a 5^a$ of $i$, $0\le i\le 5^m-2$, and $i_a\in F_5$.

It can be easily derived that

$$\binom{0}{2}=0,\quad \binom{1}{2}=0,\quad \binom{2}{2}=1,\quad \binom{3}{2}=3,\quad \binom{4}{2}=1 \mod 5.$$

In order to satisfy (14), all the $i_a$'s are larger than or equal to 2 for $0\le a\le m-1$ and the number of occurrences $i_a=3$ in the 5-adic expansion of $i$ should be a multiple of 4 because the order of element 3 in $F_5$ is 4, that is, $3^4=1 \mod 5$. That is, $i_a=3$ occurs $4j$ times and $i_a=2$ or 4 occurs $m-4j$ times in the 5-adic expansion of $i$. For $0\le i\le 5^m-2$, the number of integers $i$ satisfying (14) can be counted as

$$C=\sum_{j=0}^{\lfloor\frac{m}{4}\rfloor}\binom{m}{4j}\cdot 2^{m-4j}-1$$

where $i=5^m-1=(4,4,4,\dots,4)$ is excluded even though the number of occurrences $i_a=3$ in the 5-adic expansion of $i$ is $0 \mod 4$, because $i>5^m-2$.

Therefore, the linear complexity over $F_5$ of the LCE sequence of period $5^m-1$ is given as

$$L_5=5^m-1-C=5^m-\sum_{j=0}^{\lfloor\frac{m}{4}\rfloor}\binom{m}{4j}\cdot 2^{m-4j}. \qquad \square$$

### C. Linear Complexity Over $F_7$ of LCE Sequences of Period $7^m-1$

Similarly to the previous two cases of $p=3$ and 5, the linear complexity over $F_7$ of the LCE sequence of period $7^m-1$ is derived by counting nonzero Fourier coefficients of the sequences as in the following theorem.

*Theorem 5:* The linear complexity over $F_7$ of the LCE sequence of period $n=7^m-1$ is given as

$$L_7=7^m-\sum_{i=0}^{1}\sum_{j=0}^{2}\sum_{u=0}^{\lfloor\frac{m-i-j-k}{2}\rfloor}\sum_{v=0}^{\lfloor\frac{m-i-j-k-2u}{3}\rfloor}\cdot\sum_{w=0}^{\lfloor\frac{m-i-j-k-2u-3v}{6}\rfloor}\binom{m}{2u+i,\,3v+j,\,6w+k,\,D}$$

where $\lfloor d\rfloor$ is the largest integer less than or equal to $d$ and $D=m-2u-i-3v-j-6w-k$ and $k$, $0\le k\le 5$ is a positive integer satisfying

$$3i+4j+k=\begin{cases}0 \mod 6, & \text{if } m \text{ is even}\\ 3 \mod 6, & \text{if } m \text{ is odd.}\end{cases}$$

*Proof:* Using the relation

$$\frac{7^m-1}{2}=\begin{cases}\text{even}, & \text{if } m \text{ is even}\\ \text{odd}, & \text{if } m \text{ is odd}\end{cases} \tag{15}$$

(11) for $p=7$ can be expressed as

$$\prod_{a=0}^{m-1}\binom{i_a}{3}=\binom{i_0}{3}\cdot\binom{i_1}{3}\cdots\binom{i_{m-1}}{3}=(-1)^m \mod 7 \tag{16}$$

where $i_a\in F_7$. Using (16), the theorem can be proved in a similar manner to that of the previous theorem. $\square$

## III. Trace Representation of LCE Sequences of Period $p^m-1$

In this section, the trace representation of LCE sequences 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. For our sequences, the $A_i$'s in (5) are in $F_p$. If the Fourier coefficients $A_i$'s for all elements in a coset corresponding to the element $\alpha^i$ have the same value, then the summation of all elements in the coset makes the trace function $A_i\cdot \mathrm{tr}(\alpha^{it})$. Further, if $A_i$'s have the same values for all elements within the same cosets of $F_{p^m}$, (5) can be expressed as a linear combination of the trace functions over $F_p$ given by

$$s(t)=\sum_{a\in L}A_a\cdot \mathrm{tr}_1^{k_a}(\alpha^{at}) \tag{17}$$

where $L$ is a set of coset leaders for the set of cyclotomic cosets modulo $p^m-1$, and for each $a\in L$, $F_{p^{k_a}}$ is the smallest subfield of $F_{p^m}$ containing $\alpha^a$. Thus, it is enough to find the Fourier coefficients $A_a$'s for all coset leaders for the set of cyclotomic cosets modulo $p^m-1$ if $A_i$'s have the same values for all elements within the same coset. Let $(i_0,i_1,i_2,\dots,i_{m-1})$ be a vector corresponding to the coefficients in the $p$-adic expansion $\sum_{a=0}^{m-1}i_ap^a$ of $i$, $0\le i\le p^m-2$. It is clear that all integers corresponding to the cyclic shift of vector $(i_0,i_1,i_2,\dots,i_{m-1})$ belong to the same cyclotomic coset of $F_{p^m}$.

The trace representation of the sequences of period $p^m-1$ is derived by computing all the $A_i$ coefficients, $0\le i\le p^m-2$ in (7) for the LCE sequences in (3).

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

In order to find the trace representation of LCE sequences of period $3^m-1$, let $\alpha$ be a primitive element of the finite field $F_{3^m}$. Let $\mathrm{tr}_1^{k_a}(\alpha^{at})$ denote the trace function from $F_{3^{k_a}}$ to $F_3$, where $k_a|m$ and $F_{3^{k_a}}$ is the smallest subfield of $F_{3^m}$ such that $\alpha^a\in F_{3^{k_a}}$.

We can classify the coset leaders for the set of cyclotomic cosets modulo $3^m-1$ as follows.

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

$I_1^e$: Set of even coset leaders excluding the coset leader 0, where every digit in the 3-adic expansion of coset leader only takes the values 1 or 0; for example, $10=1+9=(1,0,1)$.

$I^o$: 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 the LCE sequence of period $3^m-1$ is given in the following theorem.

*Theorem 6:* The trace representation of the LCE sequence of period $n=3^m-1$ is given by

$$s(t)=\sum_{a_i\in I^o\setminus I_1^o}\mathrm{tr}_1^{k_{a_i}}(\alpha^{a_it})+2\cdot\sum_{a_i\in I^e\setminus I_1^e}\mathrm{tr}_1^{k_{a_i}}(\alpha^{a_it})+2\cdot\sum_{a_i\in I_1^o}tr_1^{k_{a_i}}(\alpha^{a_it}).$$

*Proof:* For the LCE sequences of period $3^m-1$, the coefficients $A_i\in F_3$, $0\le i\le 3^m-2$ defined in (7) can be rewritten as

$$A_{-i}=-(-1)^i+(-1)^{i-\frac{3^m-1}{2}}\prod_{a=0}^{m-1}\binom{i_a}{1} \mod 3. \tag{18}$$

Now, we have to find all $A_i$'s, $0\le i\le 3^m-2$ for the trace representation of the 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 (18) can be modified as follows:

$$\prod_{a=0}^{m-1} \binom{i_a}{1} = \prod_{a=0}^{m-1} i_a = (A_{-i} + (-1)^i)(-1)^{m-i} \mod 3. \quad (19)$$

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 (19), which is rewritten as

$$\prod_a i_a = (-1)^m \mod 3. \quad (20)$$

A necessary condition for (20) is that the $i_a$'s in the 3-adic expansion $\sum_a i_a 3^a$ of $i$ only take the values 1 or 2, which means that the $j_a$'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 (20) 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 occurrences 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. Therefore, 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 (19). The following two subcases are considered.

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

We can rewrite (19) as

$$\prod_a i_a = -(-1)^m \mod 3 \quad (21)$$

where all $i_a$'s in the 3-adic expansion of $i$ have to take the values 1 or 2. The number of occurrences $i_a = 2$ in the 3-adic expansion of $i$ should be odd for even $m$ and even for odd $m$, which means that the number of occurrences $i_a = 1$, $0 \le a \le m - 1$ in the 3-adic expansion of $i$ should be odd for any integer $m$. Therefore, all $j_a$'s only take the value 0 or 1 and the number of occurrences of $j_a = 1$ in the 3-adic expansion of $j$ should be odd for any integer $m$, which means that $j$ is odd. This contradicts 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):

Equation (19) can be written as

$$\prod_a i_a = 0 \mod 3. \quad (22)$$

Equation (22) means that at least one of $i_a$'s in the 3-adic expansion of $i$ has to take the value 0, which means that at least one of $j_a$'s in the 3-adic expansion of $j$ 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 (19), have to be determined, which can be easily found because we have already found all $j$'s such that $A_j = 0$ or 1. Clearly, the remaining sets of coset leaders for the set of cyclotomic cosets modulo $3^m - 1$ are $I^e \backslash I_1^e$ and $I_1^o$. □

For $p = 3$, the trace representation for LCE sequence of period 80 is given in the following example, where the trace function is defined in Theorem 6.

*Example 7:* For $n = 3^4 - 1 = 80$ and $m = 4$, the LCE sequence $s(t)$ of period 80 is obtained as

$$s(t) = 01011001110011100000011111011101001111110010101100001000101001010110110010011000.$$

The coset leaders for the set of cyclotomic cosets modulo $3^4 - 1$ can be classified as

$$\begin{aligned} I_1^o &= \{1, 13\} \\ I_1^e &= \{4, 10, 40\} \\ I^o \backslash I_1^o &= \{5, 7, 11, 17, 23, 25, 41, 53\} \\ I^e \backslash I_1^e &= \{0, 2, 8, 14, 16, 20, 22, 26, 44, 50\}. \end{aligned}$$

Then the LCE sequence $s(t)$ of period 80 can be expressed as a linear combination of trace functions over $F_3$ as follows:

$$\begin{aligned} s(t) = &\{\mathrm{tr}_1^4(\alpha^{5t}) + \mathrm{tr}_1^4(\alpha^{7t}) + \mathrm{tr}_1^4(\alpha^{11t}) + \mathrm{tr}_1^4(\alpha^{17t}) \\ &+ \mathrm{tr}_1^4(\alpha^{23t}) + \mathrm{tr}_1^4(\alpha^{25t}) + \mathrm{tr}_1^4(\alpha^{41t}) + \mathrm{tr}_1^4(\alpha^{53t})\} \\ &+ 2 \cdot \{\mathrm{tr}_1^1(\alpha^{0t}) + \mathrm{tr}_1^4(\alpha^{2t}) + \mathrm{tr}_1^4(\alpha^{8t}) + \mathrm{tr}_1^4(\alpha^{14t}) \\ &+ \mathrm{tr}_1^4(\alpha^{16t}) + \mathrm{tr}_1^2(\alpha^{20t}) + \mathrm{tr}_1^4(\alpha^{22t}) + \mathrm{tr}_1^4(\alpha^{26t}) \\ &+ \mathrm{tr}_1^4(\alpha^{44t}) + \mathrm{tr}_1^2(\alpha^{50t})\} + 2 \cdot \{\mathrm{tr}_1^4(\alpha^{t}) + \mathrm{tr}_1^4(\alpha^{13t})\} \end{aligned}$$

where $\alpha$ is a primitive element of $F_{3^4}$.

### *B. Trace Representation of LCE Sequences of Period* $5^m - 1$

For the period $5^m - 1$, the trace representation of LCE sequences is derived similarly to the case of period $3^m - 1$. Let $\alpha$ be a primitive element of the finite field $F_{5^m}$. Let $\mathrm{tr}_1^{k_a}(\alpha^{at})$ denote the trace function from $F_{5^{k_a}}$ to $F_5$, where $k_a | m$ and $F_{5^{k_a}}$ is the smallest subfield of $F_{5^m}$ such that $\alpha^a \in F_{5^{k_a}}$.

The coset leaders for the set of cyclotomic cosets modulo $5^m - 1$ 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 occurrences of 1 in the 5-adic expansion of coset leader is $1 \mod 4$.

$I_3^o$: 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 occurrences of 1 in the 5-adic expansion of coset leader is $3 \mod 4$.

$I_0^e$: Set of even coset leaders excluding coset leader 0, where every digit in the 5-adic expansion of coset leader only takes the values 0, 1, or 2 and the number of occurrences of 1 in the 5-adic expansion of coset leader is $0 \mod 4$.

$I_2^e$: Set of even 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 occurrences of 1 in the 5-adic expansion of coset leader 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 $I_2^e$.

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

*Theorem 8:* The trace representation of LCE sequence of period $n = 5^m - 1$ is given as

$$s(t) = \sum_{a_i \in I^o \setminus \{I_1^o \cup I_3^o\}} 2 \cdot \mathrm{tr}_1^{k_{a_i}}(\alpha^{a_i t}) + \sum_{a_i \in I^e \setminus \{I_0^e \cup I_2^e\}} 3 \cdot \mathrm{tr}_1^{k_{a_i}}(\alpha^{a_i t}) + \sum_{a_i \in I_1^o} \mathrm{tr}_1^{k_{a_i}}(\alpha^{a_i t}) + \sum_{a_i \in I_3^o} 3 \cdot \mathrm{tr}_1^{k_{a_i}}(\alpha^{a_i t}) + \sum_{a_i \in I_2^e} \mathrm{tr}_1^{k_{a_i}}(\alpha^{a_i t}).$$

*Proof:* For the LCE sequences of period $5^m - 1$, the coefficients $A_i \in F_5, 0 \le i \le 5^m - 2$ defined in (7) can be rewritten as

$$3A_{-i} = -(-1)^i + (-1)^{i - \frac{5^m - 1}{2}} \prod_{a=0}^{m-1} \binom{i_a}{2} \bmod 5. \tag{23}$$

Using (23), the theorem can be proved in the same manner as in the previous theorem. □

For $p = 5$, the trace representation for LCE sequence of period $124$ is given in the following example, where the trace function is defined in Theorem 8.

*Example 9:* For $n = 5^3 - 1 = 124$ and $m = 3$, the LCE sequence $s(t)$ is given as

$$\begin{gathered} 1110011110111000011100010111001 \\ 0011101001100001111111101010111 \\ 0010000000101010110100110000100 \\ 1110010000100100101101110100110. \end{gathered}$$

The coset leaders for the set of cyclotomic cosets modulo $5^3 - 1$ can be classified as follows:

$$\begin{aligned} I_1^o &= \{1, 7, 11, 37\} \\ I_3^o &= \{31\} \\ I_0^e &= \{2, 12, 62\} \\ I_2^e &= \{6, 32\} \\ I^o \setminus \{I_1^o \cup I_3^o\} &= \{3, 9, 13, 17, 19, 21, 23, 33, 39, 43, 47, 49, \\ &\qquad 63, 69, 73, 93, 99\} \\ I^e \setminus \{I_1^e \cup I_3^e\} &= \{0, 4, 8, 14, 16, 18, 22, 24, 34, 38, 42, \\ &\qquad 44, 48, 64, 68, 74, 94\}. \end{aligned}$$

Then, the LCE sequence $s(t)$ of period $124$ can be expressed as a linear combination of trace functions over $F_5$ as follows:

$$s(t) = \sum_{a_i \in I^o \setminus \{I_1^o \cup I_3^o\}} 2 \cdot \mathrm{tr}_1^{k_{a_i}}(\alpha^{a_i t}) + \sum_{a_i \in I^e \setminus \{I_0^e \cup I_2^e\}} 3 \cdot \mathrm{tr}_1^{k_{a_i}}(\alpha^{a_i t}) + \sum_{a_i \in I_1^o} \mathrm{tr}_1^{k_{a_i}}(\alpha^{a_i t}) + \sum_{a_i \in I_3^o} 3 \cdot \mathrm{tr}_1^{k_{a_i}}(\alpha^{a_i t}) + \sum_{a_i \in I_2^e} \mathrm{tr}_1^{k_{a_i}}(\alpha^{a_i t})$$

where $\alpha$ is a primitive element of $F_{5^3}$.

## References


[1] L. D. Baumert, *Cyclic Difference Sets (Lecture Notes in Mathematics)*. New York: Springer-Verlag, 1971.

[2] E. R. Berlekamp, *Algebraic Coding Theory*, revised ed. Laguna Hills, CA: Aegean Park, 1984.

[3] R. E. Blahut, "Transform techniques for error control codes," *IBM J. Res. Develop.*, vol. 23, pp. 299–315, 1979.

[4] ——, *Theory and Practice of Error Control Codes*. New York: Addison-Wesley, 1983.

[5] H. Chung and J.-S. No, "Linear span of extended sequences and cascaded GMW sequences," *IEEE Trans. Inform. Theory*, vol. 45, pp. 2060–2064, Sept. 1999.

[6] C. Ding, T. Helleseth, and W. Shan, "On the linear complexity of Legendre sequences," *IEEE Trans. Inform. Theory*, vol. 44, pp. 1276–1278, May 1998.

[7] H. Dobbertin, "Kasami power functions, permutation polynomials and cyclic difference sets," in *Proc. NATO Advanced Study Institute Workshop on Difference Sets, Sequences and Their Correlation Properties*, , Bad Windsheim, Germany, Aug. 3–14, 1998.

[8] S. W. Golomb, *Shift-Register Sequences*. San Francisco/Laguna Hills, CA: Holden- Day/Aegean Park, 1967/1982.

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

[10] D. Jungnickel, *Finite Fields*. Mannheim, Germany: B. I. Wissenschaftsverlag, 1993.

[11] J.-H. Kim and H.-Y. Song, "Characteristic polynomial and linear complexity of Hall's sextic residue sequences," in *Proc. 2001 Conf. Sequences and Their Applications (SETA '01)*, Bergen, Norway, May 13–17, 2001, pp. 33–34.

[12] A. Lempel, M. Cohn, and W. L. Eastman, "A class of binary sequences with optimal autocorrelation properties," *IEEE Trans. Inform. Theory*, vol. IT–23, pp. 38–42, Jan. 1977.

[13] R. Lidl and H. Niederreiter, "Finite fields," in *Encyclopedia of Mathematics and Its Applications*. Reading, MA: Addison-Wesley, 1983, vol. 20.

[14] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.

[15] 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, pp. 1638–1644, May 2001.

[16] J.-S. No, H. Chung, and M.-S. Yun, "Binary pseudorandom sequences of period $2^m - 1$ with ideal autocorrelation generated by the polynomial $z^d + (z+1)^d$," *IEEE Trans. Inform. Theory*, vol. 45, pp. 1278–1282, May 1999.

[17] J.-S. No, S. W. Golomb, G. Gong, H.-K. Lee, and P. Gaal, "Binary pseudorandom sequences of period $2^n - 1$ with ideal autocorrelation," *IEEE Trans. Inform. Theory*, vol. 44, pp. 814–817, Mar. 1998.

[18] 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, pp. 2254–2255, Nov. 1996.

[19] J.-S. No, K. Yang, H. Chung, and H.-Y. Song, "On the construction of binary sequences with ideal autocorrelation property," in *Proc. 1996 IEEE Int. Symp. Information Theory and Its Applications (ISITA '96)*, Victoria, BC, Canada, Sept. 17–20, 1996, pp. 837–840.

[20] R. A. Scholtz and L. R. Welch, "GMW sequences," *IEEE Trans. Inform. Theory*, vol. IT–30, pp. 548–553, May 1984.

[21] V. M. Sidelnikov, "Some $k$-valued pseudo-random and nearly equidistant codes," *Probl. Pered. Inform.*, vol. 5, no. 1, pp. 16–22, 1969.

[22] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications*, revised ed. Rockville, MD/New York: Computer Science/McGraw-Hill, 1985/1994, vol. 1.

[23] T. Storer, *Cyclotomy and Difference Sets (Lecture Notes in Advanced Mathematics)*. Chicago, IL: Markham, 1967.

[24] R. Turyn, "The linear generation of the Legendre sequences," *J. Soc. Ind. Appl. Math*, vol. 12, no. 1, pp. 115–117, 1964.