Linear Complexity over F_p and Trace Representation of Lempel-Cohn-Eastman Sequences

Tor Helleseth
Dept. Inform., Univ. Bergen,
N-5020 Bergen, Norway,
e-mail: Tor.Helleseth@ii.uib.no

Sang-Hyo Kim
School of EECS, Seoul National Univ.,
Seoul, Korea,
e-mail: kimsh@ccl.snu.ac.kr

Jong-Seon No
School of EECS, Seoul National Univ.,
Seoul, Korea,
e-mail: jsno@snu.ac.kr

Abstract — **In this paper, the linear complexity over F_p, i.e., p-rank and trace representation of Lempel-Cohn-Eastman sequences of period p^m-1 for an odd prime p is determined.**

I. Introduction

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 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 a 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 [2]

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

Let S be a set defined as[1][2] $S=\{\alpha^{2i+1}-1 \mid 0\le i\le \frac{p^m-1}{2}-1\}$, where p is an odd prime and 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*[1]. It was turned out that the LCE sequences can be expressed with indicator function and the quadratic character given by [2]

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

where the indicator function $I(x)=1$ if $x=0$ and $I(x)=0$ otherwise and $\chi(x)$ denotes the quadratic character of x.

II. Linear Complexity of LCE 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 $A_i=\frac{1}{n}\sum_{t=0}^{n-1}s(t)\alpha^{-it}$ and its inverse Fourier transform as $s(t)=\sum_{i=0}^{n-1}A_i\alpha^{it}$, where α is a primitive element of F_{p^m} and $A_i\in F_{p^m}$.

Lemma 1 : A_{-i} of the LCE sequences defined in (2) is given as

$$(p-2)A_{-i}=-(-1)^i+(-1)^{i-\frac{p^m-1}{2}}\cdot\prod_{a=0}^{m-1}\binom{i_a}{\frac{p-1}{2}} \mod p, \quad (3)$$

where i_a's are coefficients in the p-adic expansion $\sum_a i_a p^a$ of i.

To determine the linear complexity of the sequences, 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 (3). We have proved the following result.

[1]This work was supported by BK21 and ITRC program of the Korean Ministry of Information and Communications.

Theorem 2 : Let C be a number of integers i, $0\le i\le p^m-2$ satisfying the relation $\prod_{a=0}^{m-1}\binom{i_a}{\frac{p-1}{2}}=(-1)^{\frac{p^m-1}{2}} \mod p$. Then the linear complexity over F_p, *i.e.*, p-rank of the LCE sequence of period $n=p^m-1$ defined in (2) equals $L_p=n-C$.

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

Theorem 3 : The linear complexity L_3 over F_3, *i.e.*, 3-rank of the LCE sequence of period $n=3^m-1$ is given by $L_3=3^m-2^{m-1}$.

The p-ranks of LCE sequences for $p=5,7$ can also be derived.

III. Trace Representation of LCE sequences

The equation (2) can be expressed as a linear combination of the trace functions over F_p given by $s(t)=\sum_{a\in L}A_a\cdot tr_1^k(\alpha^{at})$, 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 $\alpha^a\in F_{p^k}$.

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 $\alpha^a\in F_{3^k}$. 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 in the 3-adic expansion of coset leader 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 4 : The trace representation of LCE sequence of period $n=3^m-1$ is given by

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

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 $\alpha^a\in F_{3^k}$.

The trace representation of LCE sequences for $p=5$ can also be derived.

References

[1] 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.

[2] 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.

0-7803-7501-7/02/$17.00©2002 IEEE.