On the Linear Complexity of Periodic Sequences Obtained from an M-Sequence

森内 勉 (Tsutomu MORIUCHI) *
今村 恭己 (Kyoki IMAMURA) **
上原 聡 (Satoshi UEHARA) **

∗ Dept. of Inf. and Elec. Eng., Yatsushiro National College of Technolog
Yatsushiro, Kumamoto 866, Japan
∗∗ Dept. of Comp. Sci. and Elec. Kyushu Institute of Technology
Iizuka, Fukuoka 820, Japan

Abstract

Among all the periodic sequences over $GF(q)$ of period $T = q^n - 1$, m-sequences are characterized to have the minimum linear complexity of n. In this paper periodic sequences obtained by changing ℓ, $1 \leq \ell \leq T$, symbols of an m-sequence over $GF(q)$ with period T are defined, and a simple derivation for the linear complexity L of the above mentioned sequences is described. The results show that the periodic sequences different only one symbol from the given m-sequence have the maximum linear complexity of T, and their linear complexities are in the range, $n \leq L \leq T$, which depend on the amount of ℓ and the locations of the changed symbols of ℓ in each period of the m-sequence.

1 Introduction

Let $\{a_t\}$, $t \geq 0$, be a periodic sequence over $GF(q)$ of period $T = q^n - 1$, where $q = p^m$ and p is a prime. The linear complexity (or linear span) of $\{a_t\}$ is the length of the shortest linear feedback shift register (LFSR) which can generate the infinite sequence $\{a_0, a_1, a_2, \cdots\}$. The Berlekamp-Massey algorithm [1] and the continued fraction algorithm [2],[3] are well-known for determining the linear complexity and the shortest LFSR. The linear complexity of a given sequence is considered as one of the measures for evaluating the complexity of the function or the mechanism generating it, and then means the difficulty of predictability for the sequence. In an additive stream cipher large linear complexity of the running key sequences is a necessary (but far from sufficient) condition for its practical security [4]-[6].

Hereafter let $\{a_t\}$ be an m-sequence over $GF(q)$ with period T represented as

$$a_t = \mathrm{tr}(\alpha^t), \tag{1}$$

where α is a primitive element of $GF(q^n)$, and tr() the trace function mapped onto $GF(q)$ from $GF(q^n)$ defined by

$$\mathrm{tr}(\beta) = \sum_{j=0}^{n-1} \beta^{q^j} \quad \text{for} \quad \beta \in GF(q^n). \tag{2}$$

The m-sequence above has the minimum linear complexity of n, therefore even if it has good properties of randomness, its linear complexity so small that we can not use it for the key sequence in the stream cipher. It is well known [7]-[9] that the linear complexity of the sequence can be extended by adding nonlinear operations or functions to its LFSR.

Recently, a periodic sequence $\{b_t\}$ which is obtained by changing ℓ symbols of (1) by the same amount b in each period defined by

$$b_t = \begin{cases} a_{r_i} + b & \text{if } t \equiv r_i \pmod{T} \text{ for } 0 \le i \le \ell - 1, \\ & \text{and } r_i \ne r_j \text{ if } i \ne j \\ a_t & \text{otherwise,} \end{cases} \tag{3}$$

where $b \in GF(q)\backslash\{0\}$ and $1 \le \ell \le T$, was studied on the linear complexity [10],[11]. $\{b_t\}$ has the same period T as the m-sequence, and there are $(q-1)\binom{T}{\ell}$ different $\{b_t\}$'s corresponding to $q-1$ choices of b and $\binom{T}{\ell}$ combinations of $\{r_0, r_1, \cdots, r_{\ell-1}\}$ when ℓ is fixed. And b as above can be written as

$$b = \alpha^{uT/(q-1)} \quad \text{for } 0 \le u \le q-2, \tag{4}$$

since $\alpha^{T/(q-1)}$ is a primitive element of $GF(q)$. The linear complexity L of $\{b_t\}$ defined by (3) takes any value $L \le T$, since $\{b_t\}$ can be generated by successive cyclic shift of its one period $\{b_0, b_1, \cdots, b_{T-1}\}$, so it was shown [10] that the linear complexity of (3) in the case that $\ell = 1$ becomes

$$L = \begin{cases} T-n & \text{if } r_0 = uT/(q-1) \\ T & \text{otherwise.} \end{cases} \tag{5}$$

Note that almost all the $\{b_t\}$'s as above, except $q-1$ ones from the $(q-1)T$ different $\{b_t\}$'s, have the maximum linear complexity of T much bigger than that of the m-sequence (1).

We will clarify the linear complexity of $\{b_t\}$ including the case of $\ell = 1$, which is the more general problem on the linear complexity of the sequences.

2 The Linear Complexity of the Periodic Sequence $\{b_t\}$

It is known [2],[3] that $L = \deg Q(x)$ if we find a pair of polynomials $(P(x), Q(x))$ such that $Q(x)$ is monic and of minimal degree satisfying

$$\frac{P(x)}{Q(x)} = b_0 x^0 + b_1 x^{-1} + \cdots + b_n x^{-n} + \cdots, \tag{6}$$

i.e., the coefficint of x^{-i} is equal to b_i for all $i \geq 0$. From (3) and (6) the linear complexity L of $\{b_t\}$ can be determined by the following expressions:

$$\begin{aligned}\sum_{t\geq 0} b_t x^{-t} &= \sum_{t\geq 0} a_t x^{-t} + b \sum_{k\geq 0}(\sum_{i=0}^{\ell-1} x^{-(kT+r_i)}) \\ &= \sum_{t\geq 0} \mathrm{tr}(\alpha^t)x^{-t} + \frac{b}{x^T-1}\sum_{i=0}^{\ell-1} x^{T-r_i} \qquad (7)\end{aligned}$$

as the ratio of two polynomials without a common factor. For this purpose we will use the following lemma.

Lemma 1: Let

$$f(x) = (x-\alpha^{q^0})(x-\alpha^{q^1})\cdots(x-\alpha^{q^{n-1}}) \qquad (8)$$

be the minimal polynomial of α over $GF(q)$ and $f'(x)$ the formal derivative of $f(x)$. Then we have

$$\frac{xf'(x)}{f(x)} = \sum_{t\geq 0} \mathrm{tr}(\alpha^t)x^{-t}. \qquad (9)$$

Proof: From (8) we can get

$$\begin{aligned}\frac{xf'(x)}{f(x)} &= \sum_{0\leq k\leq n-1} \frac{x}{x-\alpha^{q^k}} \\ &= \sum_{0\leq k\leq n-1} \frac{1}{1-\alpha^{q^k}x^{-1}} \\ &= \sum_{0\leq k\leq n-1} (\sum_{t\geq 0} \alpha^{tq^k}x^{-t}) \\ &= \sum_{t\geq 0}(\sum_{0\leq k\leq n-1} \alpha^{tq^k})x^{-t}, \qquad (10)\end{aligned}$$

which is equal to the right-hand side of (9).

Q.E.D.

Substitution of (9) into (7) gives

$$\begin{aligned}\sum_{t\geq 0} b_t x^{-t} &= \frac{xf'(x)}{f(x)} + \frac{b}{x^T-1}\sum_{i=0}^{\ell-1} x^{T-r_i} \\ &= \frac{F(x)}{x^T-1}, \qquad (11)\end{aligned}$$

where F(x) is a polynomial defined by

$$F(x) = \frac{(x^T-1)xf'(x)}{f(x)} + b\sum_{i=0}^{\ell-1} x^{T-r_i}. \qquad (12)$$

Here we will have to find the degree of the greatest common divisor of polynomials $(F(x), x^T - 1)$ to obtain the linear complexity of $\{b_t\}$ from (11) and (12) as well as that of (6).

Let V be a subset of v's, $0 \leq v \leq T-1$, satisfying

$$V = \{v \mid F(\alpha^v) = 0, \ \ 0 \leq v \leq T-1\}, \qquad (13)$$

and $\mid V \mid$ denotes the cardinality of V. Since all the elements of $GF(q^n)\backslash\{0\}$ are the roots that satisfy $x^T - 1 = 0$, from (11),(12) and (13) the linear complexity L of $\{b_t\}$ can be represented by

$$L = T - \mid V \mid . \qquad (14)$$

From (12) we have

$$F(\alpha^v) = b\sum_{i=0}^{\ell-1} \alpha^{-vr_i} - 1 \qquad (15)$$

for $v = q^k$, $0 \leq k \leq n-1$, and otherwise

$$F(\alpha^v) = b\sum_{i=0}^{\ell-1} \alpha^{-vr_i}, \qquad (16)$$

since in the right-hand side of (12) let

$$G(x) = \frac{(x^T - 1)xf'(x)}{f(x)},$$

then we get

$$\begin{aligned} G(\alpha^v) &= \frac{(x^T-1)x}{x-\alpha^{q^k}}\Big|_{x=\alpha^v} \\ &= \begin{cases} -1 & \text{if } v = q^k,\ 0 \le k \le n-1 \\ 0 & \text{otherwise.} \end{cases} \end{aligned} \tag{17}$$

We have to obtain $\mid V \mid$ given as (13), therefore need to solve (15) and (16) for that $F(\alpha^v) = 0$ for $0 \le v \le T-1$. Let us define the following two subsets of $V$, i.e.,

$$V_1 = \{v \mid F(\alpha^v) = 0 \text{ in } (15),\ v = q^k, 0 \le k \le n-1\}, \tag{18}$$

and

$$V_2 = \{v \mid F(\alpha^v) = 0 \text{ in } (16),\ v \ne q^k\}, \tag{19}$$

where $\mid V \mid = \mid V_1 \mid + \mid V_2 \mid$ since $\mid V_1 \cap V_2 \mid = 0$, and $\mid V_1 \mid$ takes two values either 0 or $n$. Hence from (14),(18) and (19) the linear complexity can be written by

$$L = T - \mid V_1 \mid - \mid V_2 \mid. \tag{20}$$

In general obtaining $\mid V_1 \mid$ and $\mid V_2 \mid$ from (15) and (16) in an arbitrary ℓ-tuple $\{r_0, r_1, \cdots, r_{\ell-1}\}$ is not an easy problem, especially in the case of a big order q^n, but for the following specific ℓ-tuples r_i's they will be obtained analytically.

3 The Linear Complexity of $\{b_t\}$ in Specific ℓ-Tuples r_i's

In this section we will prove the linear complexity of $\{b_t\}$ defined by (3) in specific ℓ-tuples r_i's by applying the preceding considerations.

Theorem 1: Let $\{b_t\}$ over $GF(q)$ with period T obtained from the m-sequence shown in (1) be given as

$$b_t = \begin{cases} a_{r_0+ir} + b & 0 \le i \le \ell - 1, \\ & \text{if } t \equiv r_0 + ir \pmod{T} \\ a_t & \text{otherwise,} \end{cases} \tag{21}$$

where the three parameters r, r_0 and ℓ take values $1 \le r \le T-1$, $0 \le r_0 \le T-1$, and $1 \le \ell \le T/w$ ($w = \gcd(r,T)$), respectively. If $\ell = 1$, then suppose $r = \infty$ and $\alpha^\infty = 0$.

The linear complexity L of $\{b_t\}$ is given as follows:

(1) when $r\ell \not\equiv 0(\bmod T)$,

$$L = \begin{cases} T - d + w & \text{if } \ell \not\equiv 0(\bmod p) \\ T - d - n + w & \text{if } \ell \not\equiv 0(\bmod p) \\ & \text{and satisfying (18)} \\ T - d & \text{if } \ell \equiv 0(\bmod p) \\ T - d - n & \text{if } \ell \equiv 0(\bmod p) \\ & \text{and satisfying (18),} \end{cases} \tag{22}$$

(2) when $r\ell \equiv 0(\bmod T)$,

$$L = \begin{cases} n + w & \text{if } \ell \not\equiv 0(\bmod p) \\ n & \text{if } \ell \equiv 0(\bmod p), \end{cases} \tag{23}$$

where $d = \gcd(r\ell, T)$.

Proof: By replacing r_i by $r_0 + ir$ in (15), we have

$$\begin{aligned} F(\alpha^v) &= b\sum_{i=0}^{\ell-1}(\alpha^{-r_0-ir})^{q^k} - 1 \\ &= b\alpha^{-r_0 q^k}(\frac{\alpha^{-r\ell} - 1}{\alpha^{-r} - 1})^{q^k} - 1, \end{aligned} \tag{24}$$

and then from (16) we have

$$F(\alpha^v) \;=\; b\sum_{i=0}^{\ell-1}\alpha^{(-r_0-ir)v} \text{ for } v \ne q^k,\ 0 \le k \le n-1$$

$$= \ell b\alpha^{-vr_0} \qquad \text{if } vr \equiv 0(\text{mod } T) \tag{25}$$

$$= b\alpha^{-vr_0}\frac{\alpha^{-vr\ell}-1}{\alpha^{-vr}-1} \quad \text{if } vr \not\equiv 0(\text{mod } T). \tag{26}$$

First let us obtain $\mid V_1 \mid$ from (18) and (24). Since $r \neq 0$ in (24), for that $F(\alpha^v) = 0$ we can get

$$\frac{\alpha^{-r\ell}-1}{\alpha^{-r}-1} = \alpha^{-s} \quad \text{if } r\ell \not\equiv 0(\text{mod } T), \tag{27}$$

where $\alpha^{-s} \in GF(q^n)\backslash\{0\}$, therefore substituting (27) into (24) gives

$$b\alpha^{-(r_0+s)q^k} = 1. \tag{28}$$

Then substitution of (4) for (28) gives

$$r_0 + s \equiv uT/(q-1) \ (\text{mod } T), \tag{29}$$

which follows that $v = q^k$ for $0 \leq k \leq n-1$ belong to V_1 in only one position r_0 satisfying (29). Thus we get

$$\mid V_1 \mid = \begin{cases} n & \text{if satisfying (29)} \\ 0 & \text{if not satisfying (29) or } r\ell \equiv 0(\text{mod } T). \end{cases} \tag{30}$$

Secondly let us consider $\mid V_2 \mid$ from (19),(25) and (26). From (25) if $vr \equiv 0(\text{mod } T)$ and $\ell \equiv 0(\text{mod } p)$, then v's satisfy $F(\alpha^v) = 0$

$$v = (T/w)c \quad \text{for } \ 0 \leq c \leq w-1, \tag{31}$$

where $w = \gcd(r, T)$, belong to V_2. Then since from (26) $F(\alpha^v) = 0$ implies

$$vr\ell \equiv 0 \ (\text{mod } T) \quad \text{if } vr \not\equiv 0 \ (\text{mod } T). \tag{32}$$

If $r\ell \equiv 0 (\bmod T)$, then (32) contains v's of $T - w - n$ in V_2, and when $r\ell \not\equiv 0 (\bmod T)$, the below v's satisfying (32)

$$v = (T/d)c \quad \text{for} \quad 1 \leq c \leq d - 1 \tag{33}$$

are considered as the elements in V_2, where $d = \gcd(r\ell, T)$. However when $r\ell \not\equiv 0 (\bmod T)$, the number of v's in V_2 satisfying (33) reduces to $d - w$ since v's for (31) can be included among them of (33). Thus we get the following results concerning $\mid V_2 \mid$:

(1) when $r\ell \not\equiv 0 (\bmod T)$,

$$\mid V_2 \mid = \begin{cases} d & \text{if } \ell \equiv 0 (\bmod p) \\ d - w & \text{if } \ell \not\equiv 0 (\bmod p), \end{cases} \tag{34}$$

(2) when $r\ell \equiv 0 (\bmod T)$,

$$\mid V_2 \mid = \begin{cases} T - n & \text{if } \ell \equiv 0 (\bmod p) \\ T - w - n & \text{if } \ell \not\equiv 0 (\bmod p), \end{cases} \tag{35}$$

where $w = \gcd(r, T)$ and $d = \gcd(r\ell, T)$.

We come to Theorem 1 by substitution of (30),(34) and (35) into (20). From (22) of Theorem 1 the linear complexity L of $\{b_t\}$ with $\ell = 1$(set $r = \infty$) shown in (5), where $r\ell \not\equiv 0 (\bmod T)$, $\ell \not\equiv 0 (\bmod T)$, and $d = w = \gcd(\infty, T) = 1$, can be got the same results as (5).

Q.E.D.

We confirmed that the main equations (15) and (16) for determining the linear complexity of $\{b_t\}$ defined by (3) or (21) can be also derived from Blahut's Theorem [12]. It follows that let $\{B_v\}$, $0 \leq v \leq T - 1$, be the discrete Fourier transform sequence of $\{b_t\}$

in $GF(q^n)$, then from (7), (12) and (17) they are represented by

$$\begin{aligned} B_v &= \sum_{t=0}^{T-1} b_t \alpha^{-vt} \\ &= \sum_{t=0}^{T-1} \mathrm{tr}(\alpha^t)\alpha^{-vt} + b\sum_{i=0}^{\ell-1} \alpha^{-vr_i} \\ &= \begin{cases} b\sum_{i=0}^{\ell-1} \alpha^{-vr_i} - 1 & \text{for } v = q^k \ 0 \leq k \leq n-1 \\ b\sum_{i=0}^{\ell-1} \alpha^{-vr_i} & \text{otherwise,} \end{cases} \end{aligned}$$

which are the same formulas as (15) and (16). Hence let $Wt(B)$ denote the number of nonzero elements of $\{B_v\}$ in period T, then $\mid V \mid = T - Wt(B)$ since $B_v = F(\alpha^v)$, and $L = Wt(B)$ from (14).

4 Conclusion

It was shown the linear complexity of the periodic sequences obtained by changing ℓ digits at arbitrary locations in each period of the m-sequence over $GF(q)$ of period $q^n - 1$. When the location r_i, $0 \leq i \leq \ell - 1$ where the m-sequence is changed ℓ digits in each period is represented as $r_i = r_0 + ir$ for $0 \leq r_0 \leq T-1$, and $1 \leq r \leq T-1$, the linear complexity of the sequences were described in detail.

参考文献

[1] J.L.Massey,"Shift Register Synthesis and BCH Decoding", *IEEE Trans. I.T.*, Vol.IT-15, pp.122-127, Jan. 1969.

[2] W.H.Mills,"Continued Fractions and Linear Recurrences", *Math. Comput.* Vol.29, pp.173-180,Jan. 1975.

[3] L.R.Welch and R.A.Sholtz,"Continued Fractions and Berlekamp's Algorithm", *IEEE Trans. I.T.*, Vol.IT-25, pp.19-27, Jan. 1979.

[4] R.A.Rueppel,"Analysis and Design of Stream Ciphers", *Springer-Verlag*, 1986.

[5] J.L.Massey,"An Introduction to Cryptology",*Proc. IEEE*, Vol.76, pp.533-549, May 1988.

[6] C.Ding, G.Xiao and W.Shan, *The Stability Theory of Stream Ciphers*, to be published as one of the Lecture Notes in Comp. Sci. from *Springer-Verlag.*

[7] E.L.Key,"An Analysis of the Structure and Complexity of Nonlinear Binary Sequence Generator", *IEEE Trans. on I.T.*, Vol.IT-22, No.6, pp.732-736, Nov. 1976.

[8] E.J.Groth,"Generation of Binary Sequences with Controllabl Complexity", *IEEE Trans. on I.T.*, Vol.IT-17, No.3, pp.288-296, May 1971.

[9] P.R.Geffe,"How to Protect Data with Ciphers That Are Really Hard to Break", *Electronics*, pp.99-101, Jan. 1973.

[10] K.Imamura, T.Moriuchi and S.Uehara,"On the Linear Complexity of a Periodic Sequence", *IEICE*, IT90-79, pp.27-29,Oct. 1990.

[11] K.Imamura and G.Xiao,"Periodic Sequences of the Maximum Linear Complexity and M-sequences", *The Proc. of the 15th SITA*, pp.149-151, Sep. 1992.

[12] J.L.Massey and T.Schaub,"Linear Complexity in Coding Theory ", *Lecture Notes in Comp. Science, Coding Theory and Applications, Spring-Verlag*, pp.19-31, Nov. 1986.