Linear Complexity of the Balanced Polynomial Quotients Sequences

Chun-e Zhao, Tongjiang Yan and Qihua Niu

College of Sciences, China University of Petroleum, Qingdao 266555, China

Abstract. Balanced binary sequences of large linear complexity have series applications in communication systems. In the past, although the sequences derived from polynomial quotients have large linear complexity, but they are not balanced. In this paper, we will construct new sequences which are not only with large linear complexity but also balanced. Meanwhile, this linear complexity reaches the known k-error linear complexity mentioned in [7], which means that the k-error linear complexity as a lower bound is tight.

1 Introduction

Let q be prime number $(q>2)$ and a is a number which satisfies $a \neq 0$.

The polynomial quotient (PQ) mentioned in [1] modulo q is defined as

$$F_w(a) \equiv \frac{a^w - a^{wq}}{q} (\mathrm{mod}\, q),$$

where $0 \le w, F_w(a) \le q-1$. In particular, when $w=q$-1, $F_w(a)$ is referred to Fermat quotient (FQ).

The FQ sequences have been studied by Ostafe in [2]. Then three classes of sequences have already been discussed from the view point of polynomial quotients.

One is the threshold sequence defined as

$$e_u = \begin{cases} 0, & 0 \le F_w(u) \le \dfrac{q-1}{2} \\ 1, & \dfrac{q+1}{2} \le F_w(u) < q \end{cases}, u \ge 0.$$

The second one is the Legendre PQ sequence (f_u) defined below

$$f_u = \begin{cases} 0, & \left(\dfrac{F_w(u)}{q}\right) = 1 \quad or \quad F_w(u) = 0 \\ 1, & otherwise \end{cases}, u \ge 0,$$

where $\left(\dfrac{\cdot}{q}\right)$ means the Legendre symbol.

The third is the sequence (s_u) defined by

$$s_u = \begin{cases} 0, & F_w(u) \text{ is even} \\ 1, & F_w(u) \text{ is odd} \end{cases}, u \ge 0.$$

When $w = q-1$, Gomez etc. discussed the pseudo-randomness of (f_u) in [3]. Chen etc. studied the properties of (e_u) in [4]. For both (e_u) and (f_u), Chen etc. considered the linear complexity (LC for short) when 2 is a generator of the multiplicative group $Z_{p^2}^*$ and then extend to condition $2^{p-1} \neq 1 (\mathrm{mod}\, p^2)$ in [5-7]. Later, Zhao, Ma, etc. gave the LC of (s_u) in [8]. It is obvious that these sequences are not balanced.

In this paper, a new balanced sequence (t_u) of polynomial quotients will be constructed as

$$t_u = \begin{cases} 1, & F_w(u) \in I, i \in I \subset Z_p^* \\ 0, & F_w(u) \notin I \end{cases}, u \ge 0 \qquad (1)$$

where I satisfies $|I| = \dfrac{q+1}{2}$. Our result shows that this sequence's balance is good and the LC is large.

For a $T-$periodic sequence (a_u) over finite field F_2, the polynomial

$$a(x) = a_0 + a_1 x + \cdots a_{T-1} x^{T-1} \in F_2[x]$$

is said to be the generating polynomial of (a_u).

The LC of (a_u) is referred to the smallest positive integer n which satisfies

$$a_{u+n} = c_0 a_u + c_1 a_{u+1} + \cdots + c_{L-1} a_{u+n-1} \text{ for } u \ge 0.$$

The following polynomial

$$c(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0 \in F_2[x]$$

is called the characteristic polynomial (CP) of (a_u). The one with the least degree is the minimal polynomial (MP). Then the MP of (a_u) is

$$\frac{x^T - 1}{\gcd(x^T - 1, a(x))}.$$

So the LC of (a_u) is

$$L((a_u)) = T - \deg(\gcd(x^T - 1, a(x))).$$

2 LC of the general PQ sequence

Lemma 1 ([6]): For $a \in Z_q$, denote

$$B_{(a,q)} = \{u \mid u \in Z_{q^2}, u \equiv a(\bmod q)\}$$
$$B_{(a,q,w)} = \{F_w(u) \mid u \in B_{(a,q)}\}, \text{ then}$$
$$B_{(a,q,w)} = \begin{cases} Z_q, & a \in Z_q^*, w \in Z_q^* \\ Z_q, & a = 0, w = 1 \\ 0, & a = 0, w > 1 \end{cases} \quad (2)$$

Theorem 1: Suppose (t_u) is the L^2 – period sequence defined as in Eq. (1). If 2 is the generator of $Z_{L^2}^*$, then the LC of (t_u) is

$$L((t_u)) = \begin{cases} L^2 - L, & L \equiv 3(\bmod 4) \\ L^2 - 1, & L \equiv 1(\bmod 4), w > 1 \\ L^2 - L + 1, & L \equiv 1(\bmod 4), w = 1 \end{cases}.$$

Proof. Let $f_1(x) = x^{L-1} + x^{L-2} + \cdots + 1$ and $f_2(x) = x^{L(L-1)} + x^{L(L-2)} + \cdots + x^L + 1$. Then $x^{L^2} - 1 = (x-1)$

$f_1(x)f_2(x)$ always holds. The MP of (t_u) Satisfies $m(x) \mid x^{q^2} - 1$. By Lemma 1, we get $B_{(a,L,w)} = Z_L$. Correspondingly, in every $B_{(a,L)}$, there are $|I|$ many u's such that $t_u = 1$ and $L - |I|$ many u's such that $t_u = 0$, respectively. So we have

$$\sum_{i=0}^{q-1} t_{v+iL} = \begin{cases} |I|, & \gcd(v, L) = 1 \\ |I|, & \gcd(v, L) = L, w = 1 \\ 0, & \gcd(v, L) = L, w > 1 \end{cases} \quad (3)$$

We will discuss the linear complexity of (t_u) in the following.

(1) $L \equiv 3(\bmod 4)$

For each v, by Eq. (3),

$$\sum_{k=0}^{L-1} t_{v+kL} = |I| = 0(\bmod 2).$$

So $f_2(x)$ is a CP of (t_u). Thus $m(x) \mid f_2(x)$. By the fact that 2 is the generator of $Z_{L^2}^*$, so $f_2(x)$ is irreducible over $F_2[x]$. Then $m(x) = f_2(x)$ and thus the LC of (t_u) is $L((t_u)) = L^2 - L$.

(2) $L \equiv 1(\bmod 4), w > 1$

By Eq. (1) and (3), for each $v \in Z_{q^2}$, we have

$$\sum_{a=0}^{L^2-1} t_{v+a} = \sum_{a=0}^{L^2-1} t_a = \sum_{t=0}^{L-1} t_{tL} + \sum_{l=1}^{L-1}\sum_{t=0}^{L-1} t_{l+tL} = (L-1)|I| = 0$$

So $f_1(x)f_2(x)$ is the CP of (t_u). So $m(x) \mid f_1(x)f_2(x)$. Since $f_1(x)$ and $f_2(x)$ are irreducible in $F_2[x]$ and neither of them is the characteristic polynomial of (t_u). Hence we can get $m(x) = f_1(x)f_2(x)$. Then the LC of (t_u) is $L((t_u)) = L^2 - 1$.

(3) $L \equiv 1(\bmod 4), w = 1$

By Eq. (3), for each v, we have

$$\sum_{k=0}^{q-1} t_{v+kq} + \sum_{k=0}^{q-1} t_{(v+1)+kq} = |I| + |I| = 0.$$

So $f_2(x) + xf_2(x) = (1+x)f_2(x)$ is the CP of (t_u). Only $(1+x)$ and $f_2(x)$ are irreducible in $F_2[x]$ but them are not the CPs of (t_u). So $m(x) = (1+x)f_2(x)$ holds. Then the LC of (t_u) is $L((t_u)) = L^2 - L + 1$.

3 LC of the special PQ sequences

In this section, we will extend to $2^{q-1} \neq 1(\bmod q^2)$ and present the LC of (t_u) when $w = q - 1$.

In the following, denote d the order of 2 modulo q^2, i.e. $2^d \equiv 1(\bmod q^2)$, F_{2^d} is a finite field with order 2^d and $\beta \in F_{2^d}$ is a primitive q^2-th root of unity. We define $H_w(u) = u^{-w}F_w(u)(\bmod q), 0 \le H_w(u) \le q-1$. We have

$$H_w(uv) \equiv H_w(u) + H_w(v)(\bmod q),$$

if $\gcd(uv, q) = 1$.

For $0 \le l < q$, let $D_l = \{u \in Z_{q^2}^* : H_w(u) = l\}$ and $aD_l = \{au(\bmod q^2) \mid u \in D_l\}$. It is easy to see that

$|D_l| = q-1$ and $aD_l = D_{l+l'}$ if $a \in D_{l'}$. Let $D_l^{mq} = \{u(\bmod q) : u \in D_l\} \subseteq Z_q$, we have $D_l^{mq} = Z_q^*$.

For $0 \le l < q$, write $D_l(x) = \sum_{u \in D_l} x^u \in F_2[x]$ and $\Omega_l(x) = \sum_{i \in I} \sum_{u \in D_{i+l}} x^u \in F_2[x]$. Let $t(x) = \sum_{u=0}^{q^2-1} t_u x^u$ be the GP of (t_u).

Lemma 2 ([5]): Suppose is a primitive q^2 − th root of unity. For every $a \in Z_{q^2}^*$, we have

$$\sum_{l=0}^{q-1} D_l(\beta^a) = 0 .$$

Lemma 3: Suppose $\beta \in F_{2^d}$ is a generator of $Z_{q^2}^*$, (t_u) is the q^2 − period sequence defined as in Eq. (1), then we have

$$t(\beta^{kq}) = \begin{cases} 0, & k = 0 \\ \frac{q+1}{2} (\bmod 2), & k = 1, \cdots, q-1 \end{cases} .$$

Proof. By Eq. (1) and the definition $t(x)$, we have

$$t(x) = \sum_{l \in I} \sum_{u \in D_l} x^u$$

For $k = 0$, we have

$$t(\beta^0) = t(1) = \sum_{l \in I} \sum_{u \in D_l} 1 = |I||D_l| = \frac{q^2-1}{2} = 0 .$$

For $k = 1, 2, \cdots, p-1$, by the fact $\beta^{q^2} = 1$, so $\beta^{kqa} = \beta^{kqu}$, where $a \equiv u(\bmod q)$. Thus

$$t(\beta^{kq}) = \sum_{l \in I} \sum_{u \in D_l} \beta^{kqu} = \sum_{l \in I} \sum_{a \in D_l^{mq}} \beta^{kqa} .$$

For the reason that $\sum_{a \in Z_q} \beta^{kqa} = 0$, we get

$$\sum_{a \in D_l^{mq}} \beta^{kqa} = \sum_{a \in Z_q^*} \beta^{kqa} = 1$$

and hence $t(\beta^{kq}) = \sum_{l \in I} 1 = |I| = \frac{q+1}{2} (\bmod 2)$.

Definition 1: The $n-$ th order matrix with the following form

$$A = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \cdots & a_{n-2} \\ a_{n-2} & a_{n-1} & a_0 & \cdots & a_{n-3} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_1 & a_2 & a_3 & \cdots & a_0 \end{pmatrix}$$

is called a cyclic matrix for $a_0, a_1, \cdots, a_{n-1}$ and is noted by $A = cir(a_0, a_1, \cdots, a_{n-1})$.

Lemma 4: The sufficient and necessary condition for the $n-$ th cyclic matrix A inverse is

$$\gcd(f(x), x^n - 1) = 1 ,$$

where

$$A = cir(a_0, a_1, \cdots, a_{n-1}) , f(x) = a_0 + \cdots + a_{n-1} x^{n-1} .$$

Lemma 5: If $2^{q-1} \ne 1 (\bmod q^2)$, then $t(\beta^a) \ne 0$ for each $a \in Z_{q^2}^*$.

Proof. According to the expression of $H_{q-1}(a)$, when $a = 2$, there exists a number k satisfying

$$H_{q-1}(2) = \frac{2^{q-1}-1}{q} + kq ,$$

which implies the following equation.

$$2^{q-1} = H_{q-1}(2) q + 1 (\bmod q^2) .$$

By the fact $2^{q-1} \ne 1 (\bmod q^2)$, so $H_{q-1}(2) \ne 0$. Let $H_{q-1}(2) = l_0 (1 \le l_0 < q)$ and $2 \in D_{l_0}$. We obtain $2^j \in D_{jl_0 (\bmod q)}$.

Suppose $h(\beta^{n_0}) = 0$ for some $n_0 \in Z_{q^2}^*$ and $n_0 \in D_{i_0}$. Then

$$0 = h(\beta^{n_0})^{2^j} = h(\beta^{n_0 2^j}) = \Omega_{i_0 + jl_0}(\beta) .$$

Because $\gcd(l_0, q) = 1$, then $i_0 + jl_0$ takes every value in Z_q when j turns over $\{0, 1, \cdots, q-1\}$, which indicate that for each pair $j \in Z_q$, $m \in Z_q^*$, $\Omega_j(\beta) = 0$ and $\Omega_j(\beta^m) = 0$ always holds. Then we get the following equation system:

$$\begin{cases} \Omega_0(\beta^m) = \sum_{i \in I} \sum_{u \in D_l} (\beta^m) = 0 \\ \Omega_1(\beta^m) = \sum_{i \in I} \sum_{u \in D_{i+1}} (\beta^m) = 0 \\ \Omega_2(\beta^m) = \sum_{i \in I} \sum_{u \in D_{i+2}} (\beta^m) = 0 \\ \cdots\cdots\cdots\cdots \\ \Omega_{q-1}(\beta^m) = \sum_{i \in I} \sum_{u \in D_{i+q-1}} (\beta^m) = 0 \end{cases}$$

Denote $\gamma = (c_0, c_1, \cdots, c_{q-1})$, where $c_i = \begin{cases} 0, & i \notin I \\ 1, & i \in I \end{cases}$.

So the above system can be represented as

$$\begin{pmatrix} c_0 & c_1 & c_2 & \cdots & c_{q-1} \\ c_{q-1} & c_0 & c_1 & \cdots & c_{q-2} \\ c_{q-2} & c_{q-1} & c_0 & \cdots & c_{q-3} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ c_1 & c_2 & c_3 & \cdots & c_0 \end{pmatrix} \begin{pmatrix} D_0(\beta^n) \\ D_1(\beta^n) \\ D_2(\beta^n) \\ \vdots \\ D_{q-1}(\beta^n) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

The coefficient matrix B is a circular matrix. Let $f(x)=\sum_{i=0}^{q-1} c_i x^i$. Because of $|I|=\frac{q+1}{2}$, so $f(x)\neq x-1$ and $f(x)\neq x^{q-1}+\cdots+x+1$. Moreover, $\gcd(f(x),x^q-1)=1$, then B is reversible, so $BX=0$ has only zero solution.

We get $D_l(\beta^n)=0$ for all $0\le l\le q-1$. That is, for any $l=0,1,\cdots,q-1$, there are at least $q(q-1)$ many $i's$ in $Z_{q^2}^*$ such that $D_l(\beta^i)=0$. Then

$$\deg(D_l(x))\ge q(q-1)$$

holds. Let $\deg(D_l(x))=d_l$. Then d_l satisfies

$$q(q-1)\le d_l\le q^2-1.$$

Because the degrees of these $D_l(x)$'s are not the same with the others. So we have

$$\{d_l \mid 0\le l\le q-1\}=\{q^2-1,q^2-2,\cdots,q^2-q\}.$$

In fact, $q^2-q\notin Z_{q^2}^*$. This contracts with the definition of $D_l(x)$. Therefore, for every $n\in Z_{q^2}^*$, $t(\beta^n)\neq 0$.

Theorem 2 Suppose (t_u) is the sequence defined in Eq. (1) with $w=q-1$. Assume

$2^{q-1}\neq 1(\mathrm{mod}\, q^2)$, then,

$$L((t_u))=\begin{cases} q^2-1, & q\equiv 1(\mathrm{mod}\,4) \\ q^2-q, & q=3(\mathrm{mod}\,4) \end{cases}$$

Proof. Case 1: $q\equiv 1(\mathrm{mod}\,4)$

By Lemmas 3-4, only $n=0$ satisfies $t(\beta^n)=0$. So there is one common root of $t(x)$ and $x^{q^2}-1$. Then the linear complexity of (t_u) is $L((t_u))=q^2-1$.

Case 2: $q\equiv 3(\mathrm{mod}\,4)$

By Lemmas 3-4 again, we have the following results.

For every $n\in\{kq:0\le k\le q-1\}$, $t(\beta^n)=0$.

For any $n\in Z_{q^2}^*$, $t(\beta^n)\neq 0$. Then the LC of (t_u) is

$$L((t_u))=q^2-q.$$

References

1. Z. Chen, A. Winterhof, A. character sums of polynomial quotients, Contemporary Mathehatics, 2012, 579.
2. A. Ostafe, I. E. Shparlinski., Pseudorandomness and dynamics of Fermat quotients, SIAM J. Discrete Mathehatics, 201125 (1): 50-71.
3. D. Gomez, A. Winterhof, Multiplicative character sums of fermat quotients and pseudorandom sequences, Periodica Mathematica. Hungarica, 2012, 64 (2): 161-168.
4. Z. Chen, A. Ostafe, A. Winterhof, Structure of pseudorandom numbers derived from Fermat quotients, Lecture Notes in Computer Science, 2010, 6087: 73-85.
5. Z. Chen, X. Du, On the linear complexity of binary threshold sequences derived from Fermat quotients, Des. Codes and Crypt., 2013, 67 (3): 317-323.
6. Z. Chen and D. Gomez, Linear complexity of binary sequences derived from polynomial quotients, Sequences and their applications-SETA 2012, 7th international conference: 181-189.
7. Z. Chen, Z. Niu, C. Wu, On the k-error linear complexity of binary sequences derived from polynomial quotients, Sci. China Inf. Sci., 2015, doi:10.1007/s11432-014-5220-7.
8. C. Zhao, W. Ma, T. Yan, Y. Sun. Linear complexity of least significant bit of polynomial quotients, Chinese Journal of Electronics, 2017, 26 (3):. 573-578.