AN EXTENSION OF BINARY THRESHOLD SEQUENCES
FROM FERMAT QUOTIENTS

XIAONI DU
College of Mathematics and Statistics, Northwest Normal University
Lanzhou, Gansu 730070, China

and

State Key Lab. of Integrated Service Networks, Xidian University
Xi’an, Shaanxi 710071, China

CHENHUANG WU
School of Mathematics, Putian University
Putian, Fujian 351100, China

WANYIN WEI
College of Mathematics and Statistics, Northwest Normal University
Lanzhou, Gansu 730070, China

(Communicated by Ding Cunsheng)

Abstract. We extend the construction of \( p^2 \)-periodic binary threshold sequences derived from Fermat quotients to the \( d \)-ary case where \( d \) is an odd prime divisor of \( p - 1 \), and then by defining cyclotomic classes modulo \( p^2 \), we present exact values of the linear complexity under the condition of \( d^{p-1} \not\equiv 1 \pmod{p^2} \). Also, we extend the results to the Euler quotients modulo \( p^r \) with odd prime \( p \) and \( r \geq 2 \). The linear complexity is very close to the period and is of desired value for cryptographic purpose. The results extend the linear complexity of the corresponding \( d \)-ary sequences when \( d \) is a primitive root modulo \( p^2 \) in earlier work. Finally, partial results for the linear complexity of the sequences when \( d^{p-1} \equiv 1 \pmod{p^2} \) is given.

1. Introduction

For an odd prime \( p \) and an integer \( u \) with \( \gcd(u, p) = 1 \), the Fermat quotient \( q_p(u) \) modulo \( p \) is defined as the unique integer with

\[
q_p(u) \equiv \frac{u^{p-1} - 1}{p} \pmod{p}, \quad 0 \leq q_p(u) \leq p - 1.
\]

More recently, Fermat quotients are studied from the viewpoint of cryptography, see [3,4,9,11,16]. Exactly speaking, Fermat quotients are used to construct pseudorandom sequences. And certain cryptographic measures, such as correlation measure and linear complexity, are also studied in the above literatures.

In particular, after adding the definition of

\[
q_p(kp) = 0, \quad k \in \mathbb{Z},
\]

2010 Mathematics Subject Classification: Primary: 94A55, 94A60; Secondary: 65C10.

Key words and phrases: Euler quotients, Fermat quotients, pseudorandom sequences, linear complexity, cryptography.
Chen, Ostafe and Winterhof defined binary threshold sequences \((e_u)\) in [4] by
\[
e_u = \begin{cases} 
0, & \text{if } 0 \leq q_p(u)/p < \frac{1}{2}, \\
1, & \text{if } \frac{1}{2} \leq q_p(u)/p < 1,
\end{cases} 
0 \leq u \leq p^2 - 1.
\]
The linear complexity (see below for the definition) of \((e_u)\) was studied in [2].

Considering the application of \(d\)-ary sequences in many fields, we extend the binary sequences above to define
\[
f_u = \begin{cases} 
0, & \text{if } 0 \leq q_p(u) \leq \ell, \\
1, & \text{if } \ell + 1 \leq q_p(u) \leq 2\ell, \\
\vdots & \\
d - 1, & \text{if } (d - 1)\ell + 1 \leq q_p(u) \leq p - 1,
\end{cases}
\]
where \(d\) is a prime and \(d| (p - 1)\) and \(\ell = (p - 1)/d\). In fact, if \(d = 2\), \((f_u)\) is the binary threshold sequence in (1).

Below we will calculate the linear complexity of \((f_u)\). The linear complexity is considered as a primary quality measure for periodic sequences and plays an important role in applications of sequences in cryptography. A low linear complexity has turned out to be undesirable for cryptographical applications. We recall that the linear complexity \(L((s_u))\) of a \(T\)-periodic sequence \((s_u)\) with terms in the finite field \(\mathbb{F}_q\) with \(q\) elements is the least order \(L\) of a linear recurrence relation over \(\mathbb{F}_q\)
\[s_u + L + c_{L-1}s_{u+L-1} + \ldots + c_1s_{u+1} + c_0s_u = 0 \quad \text{for } u \geq 0\]
which is satisfied by \((s_u)\) and where \(c_0 \neq 0, c_1, \ldots, c_{L-1} \in \mathbb{F}_q\). The polynomial
\[M(x) = x^T + c_{L-1}x^{L-1} + \ldots + c_0 \in \mathbb{F}_q[x]\]
is called the minimal polynomial of \((s_u)\). The generating polynomial of \((s_u)\) is defined by
\[S(x) = s_0 + s_1x + s_2x^2 + \ldots + s_{T-1}x^{T-1} \in \mathbb{F}_q[x].\]
It is easy to see that
\[M(x) = (x^T - 1)/\gcd(x^T - 1, S(x)),\]
hence
\[L((s_u)) = T - \deg(\gcd(x^T - 1, S(x))),\]
which is the degree of the minimal polynomial, see [14, 17] for a more detailed exposition.

2. Linear Complexity of \((f_u)\)

If we define
\[D_l = \{u : 0 \leq u \leq p^2 - 1, \; \gcd(u, p) = 1, \; q_p(u) = l\}\]
for \(l = 0, 1, \ldots, p - 1\) and let \(P = \{kp : 0 \leq k \leq p - 1\}\), \((f_u)\) can be defined equivalently by
\[
f_u = \begin{cases} 
0, & \text{if } u \in D_0 \cup \ldots \cup D_{\ell} \cup P, \\
1, & \text{if } u \in D_{\ell+1} \cup \ldots \cup D_{2\ell}, \\
\vdots & \\
d - 1, & \text{if } u \in D_{(d-1)\ell+1} \cup \ldots \cup D_{p-1},
\end{cases}
0 \leq u \leq p^2 - 1.
\]
It is easy to see that \((f_u)\) is \(p^2\)-periodic since
\[q_p(u + kp) \equiv q_p(u) - ku^{-1} \pmod p, \; \gcd(u, p) = 1.\]
Theorem 2.1. Let \((f_u)\) be the \(p^2\)-periodic \(d\)-ary sequence defined as in (2). If \(d^{p-1} \not\equiv 1 \pmod{p^2}\), then the linear complexity \(L((f_u))\) and the minimal polynomial \(m_f(x)\) of \((f_u)\) are given by
\[
L((f_u)) = p^2 - p
\]
and
\[
m_f(x) = (x^{p^2} - 1)/(x^p - 1)
\]
respectively.

Define
\[
D_l(x) = \sum_{u\in D_l} x^u \in \mathbb{F}_d[x]
\]
for \(0 \leq l \leq p - 1\). From the definition of \((f_u)\), we see that the generating polynomial of \((f_u)\) is
\[
E(x) = \sum_{u=0}^{p^2-1} f_u x^u = \sum_{j=1}^{d-1} \sum_{i=j\ell+1} x D_\ell(x) \in \mathbb{F}_d[x].
\]

Let \(\mathbb{F}_d\) be the algebraic closure of finite fields \(\mathbb{F}_d\) and \(\theta \in \mathbb{F}_d\) be a primitive \(p^2\)-th root of unity. Below we will consider the common roots of \(E(x)\) and \(x^{p^2} - 1\) in \(\mathbb{F}_d\). The number of the common roots will imply the values of linear complexity of \((f_u)\) by (3). The following lemmas are essential to the proof of Theorem 2.1.

Lemma 2.2. (i) For any \(D_l\), let \(aD_l = \{ax \pmod{p^2} : x \in D_l\}\). If \(a \in D_\ell\), then
\[
aD_l = D_{l+\ell} \pmod{p^2}.
\]
(ii) If \(a, \overline{a} \in D_l\) for some \(0 \leq l \leq p - 1\), then \(D_l(\theta^a) = D_l(\theta^{\overline{a}})\) and \(E(\theta^a) = E(\theta^{\overline{a}})\).
(iii) If \(a \in D_\ell\), then \(D_l(\theta^a) = D_{l+\ell}(\theta)\).
(iv) For all \(a \in \mathbb{Z}_{p^2}^*\), we have \(\sum_{l=0}^{p-1} D_l(\theta^a) = 0\).

Proof. (i) It’s a straight result by Lemma 1 in [2].
(ii) The results can be obtained by the definitions of \(D_l(x)\) and \(E(x)\).
(iii) It’s a straight result from (i) and the definition of \(D_l(x)\).
(iv) Since \(\theta\) is a primitive \(p^2\)-th root of unity, i.e., \(\theta^{p^2} = 1\), we have
\[
\sum_{u=0}^{p^2-1} \theta^{au} = \frac{1 - \theta^{ap^2}}{1 - \theta^a} = \frac{1 - (\theta^{p^2})^a}{1 - \theta^a} = 0
\]
and
\[
\sum_{j=0}^{p-1} \theta^{apj} = \frac{1 - \theta^{ap^2}}{1 - \theta^a} = 0.
\]

Then we derive
\[
\sum_{l=0}^{p-1} D_l(\theta^a) = \sum_{u \in \mathbb{Z}_{p^2}^*} \theta^{au} = \sum_{u=0}^{p^2-1} \theta^{au} - \sum_{j=0}^{p-1} \theta^{apj} = 0.
\]

Lemma 2.3. If \(d^{p-1} \not\equiv 1 \pmod{p^2}\), we have
\[
D_l(\theta^a) \neq 0
\]
holds for all \(0 \leq l \leq p - 1\) and all \(a \in \mathbb{Z}_{p^2}^*\).
Proof. Denote by $\lambda$ the multiplicative order of $d$ modulo $p^2$. We note here that $\lambda|p(p - 1)$. According to the definition of Fermat quotients, we have

$$d^{p-1} \equiv 1 + q_p(d)p \quad (\text{mod } p^2).$$

Since $d^{p-1} \not\equiv 1 \pmod{p^2}$, we have $q_p(d) \neq 0$ and hence $\lambda \nmid (p - 1)$. So $\lambda \geq p$ and $d^i \not\equiv d^j \pmod{p^2}$ for $0 \leq i < j \leq p - 1$. Suppose $d \in D_{d_0}$ for some $1 \leq d_0 \leq p - 1$.

By (i) of Lemma 2.2, $d^i \pmod{p^2} \in D_{d_{i_0}} \pmod{p}$ for all $0 \leq i \leq p - 1$ and

$$D_0 \cup dD_0 \cup \ldots \cup d^{p-1}D_0 = D_0 \cup D_1 \cup \ldots \cup D_{p-1} = \mathbb{Z}^*_{p^2}.$$

Moreover, the minimal polynomial of $\theta^n$ over $\mathbb{F}_d$ is given by $m(x) = \prod_{k=0}^{\lambda-1} (x - \theta^k)$. Consequently, if there are some $0 \leq l' \leq p - 1$ and some $a \in D_k$ such that $D_{l'}(\theta^n) = 0$, then $D_{l'}(\theta^{a_0}) = 0$ for $0 \leq t \leq \lambda - 1$. With (ii) of Lemma 2.2 and the definition of $< D_{d_0 } >$ we have

$$D_{l'}(\theta^n) = 0 \quad \text{for all } u \in \mathbb{Z}^*_{p^2}$$

due to the fact that

$$D_k \cup dD_k \cup \ldots \cup d^{p-1}D_k = \mathbb{Z}^*_{p^2}.$$

Furthermore, (iii) of Lemma 2.2 leads to that $D_{l'}(\theta^n) = D_{l'+1}(\theta^n)$ for some $a' \in D_{k-1}$, we also have $D_{l'+1}(\theta^n) = 0 \quad \text{for all } u \in \mathbb{Z}^*_{p^2}$. Proceed this process continually, we will get that

$$D_l(\theta^n) = 0 \quad \text{for all } 0 \leq l \leq p - 1 \quad \text{and } u \in \mathbb{Z}^*_{p^2}.$$ 

That is, for any $l = 0, 1, \ldots, p - 1$, the polynomial $D_l(x)$ has at least $p(p - 1)$ many roots. However, in the set $\{u : 0 \leq u \leq p^2 - 1, \gcd(u, p) = 1\}$ there are only $p - 1$ many elements, which appear in $D_l(x)$ as exponents for all $0 \leq l \leq p - 1$, larger than $p^2 - p$. (Notice that $x^{p^2-p}$ never appears.) So by the pigeonhole principle, there exists at least one $0 \leq l' \leq p - 1$, such that $\text{deg}(D_{l'}(x)) < p^2 - p$. This is a contradiction to the fact that the polynomial $D_{l'}(x)$ has at least $p^2 - p$ many different roots. Therefore, for all $u \in \mathbb{Z}^*_{p^2}$, we always have $D_l(\theta^n) \neq 0$. \hfill \Box

Now we prove Theorem 2.1.

Proof of Theorem 2.1. We prove this theorem by the following two facts.

(i) If $d^{p-1} \not\equiv 1 \pmod{p^2}$, then $E(\theta^u) \neq 0$ if $u \in \mathbb{Z}^*_{p^2}$.

Suppose that there is some $a \in D_{k}$ for some $0 \leq k \leq p - 1$ such that $E(\theta^n) = 0$, similar to the proof of Lemma 2.3, we have $E(\theta^n) = 0$ holds for all $u \in \mathbb{Z}^*_{p^2}$. Then we get $E(\theta^n) = E(\theta) = 0$ where $a' \in D_{k}$. It follows from (ii) and (iii) of Lemma 2.2 and after a simple calculation that

$$E(\theta^n) = \sum_{j=0}^{d-1} (j - 1) \sum_{i=0}^{(j+1)p} D_i(\theta) = D_0(\theta) + D_1(\theta).$$

Thus, we have

$$0 = -D_1(\theta) = E(\theta) = E(\theta^n) = \sum_{j=0}^{p-1} D_j(\theta) - D_1(\theta)$$

by (iv) of Lemma 2.2. This contradicts Lemma 2.3. Therefore, for all $u \in \mathbb{Z}^*_{p^2}$, we always have $E(\theta^n) \neq 0$.

(ii) $E(\theta^n) = 0$ if $u = kp$, $k = 0, \ldots, p - 1$.
Note the fact that each $D_l$ has $p - 1$ many elements for $0 \leq l < p$ and $D_l \pmod{p} = \{1, 2, \ldots, p - 1\}$ (see proof of Lemma 3 in [2]). So we have the following two results.

If $u = 0$, we have

$$E(\theta^0) = E(1) = \sum_{j=1}^{d-1} \sum_{i=j+1}^{(j+1)\ell} D_i(1)$$

$$= \sum_{j=1}^{d-1} \sum_{i=j+1}^{(j+1)\ell} (p-1) - \sum_{j=1}^{d-1} j \ell$$

$$\equiv 0 \pmod{d}$$

and if $u = kp$ for $1 \leq k \leq p - 1$, we find

$$E(\theta^u) = \sum_{j=1}^{d-1} \sum_{i=j+1}^{(j+1)\ell} D_i(\theta^{kp})$$

$$= \sum_{j=1}^{d-1} \sum_{i=j+1}^{(j+1)\ell} (\theta^{pk} + \theta^{2pk} + \ldots + \theta^{(p-1)pk})$$

$$= \sum_{j=1}^{d-1} \sum_{i=j+1}^{(j+1)\ell} (-1) = -\ell \cdot \sum_{j=1}^{d-1} j$$

$$\equiv 0 \pmod{d}$$

Putting everything together, we have $E(\theta^u) = 0$ if and only if $u \in \{kp : 0 \leq k \leq p - 1\}$, that is, the number of the common roots of $E(x)$ and $x^{p^2} - 1$ is $p$, so the linear complexity of $(f_u)$ is $p^2 - p$ by (3). Meanwhile, it is easy to see that the minimal polynomial $m_f(x)$ of $(f_u)$ satisfies $m_f(x) = (x^{p^2} - 1)/(x^p - 1)$.

To illustrate the validity of Theorem 2.1, some examples of $p^2$-periodic $d$-ary sequences $(f_u)$ are given as follows:

| $p$ | $d$ | $L((f_u))$ | $L((f_u))$ satisfying |
|-----|-----|------------|----------------------|
| 7   | 3   | 42         | $p^2 - p$            |
| 11  | 5   | 110        | $p^2 - p$            |
| 13  | 3   | 156        | $p^2 - p$            |
| 19  | 3   | 342        | $p^2 - p$            |
| 23  | 11  | 506        | $p^2 - p$            |
| 29  | 7   | 812        | $p^2 - p$            |
| 31  | 3 or 5 | 930    | $p^2 - p$            |
| 43  | 3 or 7 | 1806   | $p^2 - p$            |

3. Extension

For an odd prime $p$, integers $r \geq 2$ and $u$ with $\gcd(u, p) = 1$, the Euler quotient $Q_{p^r}(u)$ modulo $p^r$ is defined as the unique integer with

$$Q_{p^r}(u) \equiv \frac{\varphi(p^r) - 1}{p^r} \pmod{p^r}, \quad 0 \leq Q_{p^r}(u) \leq p^r - 1,$$

where $\varphi(-)$ is the Euler totient function, and we also define

$$Q_{p^r}(kp) = 0, \quad k \in \mathbb{Z}.$$

See, e.g., [1, 5, 18] for details. We note that $Q_{p^r}(u)$ is a $p^{r+1}$-periodic sequence modulo $p^r$ by the fact

$$Q_{p^r}(u + kp^r) \equiv Q_{p^r}(u) - kp^{r-1}u^{-1} \pmod{p^r}$$
for any integers $k$ and $u$ with $\text{gcd}(u,p) = 1$.

We note that $Q_p^{\nu}(u)$ is an extension of the Fermat quotient $q_p(u)$ studied in [10,12,16,19–22] and references therein.

We define the $d$-ary sequences $(h_u)$ by

$$h_u = \begin{cases} 
0, & \text{if } 0 \leq Q_p^{\nu}(u) \leq \ell M_r, \\
1, & \text{if } \ell M_r + 1 \leq Q_p^{\nu}(u) \leq 2\ell M_r, \\
\vdots & \vdots \\
d-1, & \text{if } (d-1)\ell M_r + 1 \leq Q_p^{\nu}(u) \leq p^r-1,
\end{cases}$$

where $\ell := (p-1)/d.$ and $M_r := p^{r-1} + \ldots + p + 1 = \frac{p^r-1}{p-1}.$ One can easily see that the sequences defined in $(5)$ are the same as in $(1)$ and $(2)$ if $d = 2,$ $r = 1$ and $d > 2,$ $r = 1$ respectively. Thus, in the following, we will discuss the linear complexity of the sequences with restriction $d > 2$ and $r > 1.$ For these sequences, we have

**Theorem 3.1.** Let $(h_u)$ be the $p^{r+1}$-periodic $d$-ary sequence defined as in Eq. $(5).$ If $d^{n-1} \not\equiv 1 \pmod{p^r},$ then the linear complexity $L((h_u))$ and the minimal polynomial $m_h(x)$ of $(h_u)$ satisfy

$$L((h_u)) = p^{r+1} - p$$

and

$$m_h(x) = (x^{p^{r+1}} - 1)/(x^p - 1)$$

respectively.

In order to determine the linear complexity of the sequences, we will define a partition of the residue class ring modulo $p^{n+1}$ with respect to the Euler quotient $Q_p^{\nu}(u)$ for $1 \leq n \leq r.$

Let $D_l^{(n)} = \{ u : 0 \leq u \leq p^{n+1} - 1, \text{gcd}(u,p) = 1, Q_p^{\nu}(u) = l \}$

for $l = 0, 1, \ldots, p^n - 1$ and $n \geq 1.$ Thus, one can define $(h_u)$ equivalently by

$$h_u = \begin{cases} 
0, & \text{if } u \in D_0^{(r)} \cup \ldots \cup D_{\ell M_r}^{(r)} \cup p\mathbb{Z}_{p^r}, \\
1, & \text{if } u \in D_{\ell M_r+1}^{(r)} \cup \ldots \cup D_{2\ell M_r}^{(r)}, \\
\vdots & \vdots \\
d-1, & \text{if } u \in D_{(d-1)\ell M_r+1}^{(r)} \cup \ldots \cup D_{p^r-1}^{(r)},
\end{cases}$$

where $p\mathbb{Z}_{p^r} = \{ pa \pmod{p^r} : a = 0, 1, \ldots, p^r - 1 \}.$

Define

$$D_l^{(n)}(x) = \sum_{u \in D_l^{(n)}} x^u \in \mathbb{F}_d[x]$$

for $n = 1, 2, \ldots, r$ and $l = 0, 1, \ldots, p^n - 1,$ then the generating polynomial of $(h_u)$ is

$$H(x) = \sum_{u=0}^{p^{r+1}-1} h_u x^u = \sum_{j=1}^{d-1} \sum_{l=j\ell M_r+1}^{(j+1)\ell M_r} D_l^{(r)}(x) \in \mathbb{F}_d[x].$$

Since the proof is similar to that of the analogous conclusions about the sequence $(f_u)$ proved in Section 2, we just give a sketch. Let $\beta \in \mathbb{F}_d$ be any primitive $p^{r+1}$-th root of unity, then $\beta^{p^{r-n}} \in \mathbb{F}_d$ is a primitive $p^{n+1}$-th root of unity for all integer $n \geq 1.$ We prove this theorem by the following lemmas.
Lemma 3.2. (i) (a). For \( n' \geq n \geq 1 \) and \( 0 \leq l' \leq p^{n'} - 1 \),
\[
\{ u \pmod{p^{n+1}} : u \in D_{l'}^{(n')} \} = D_{l'}^{(n)} \pmod{p^{n}}.
\]
(b). For \( n \geq 1 \) and \( 0 \leq l \leq p^n - 1 \),
\[
\{ u \pmod{p} : u \in D_l^{(n)} \} = \{1, 2, \ldots, p - 1\}.
\]
(c) The cardinality of \( D_l^{(n)} \) is \( p - 1 \) for \( 0 \leq l < p^n \).
(ii) For all \( n \geq 1 \), let \( uD_l^{(n)} = \{ uv \pmod{p^{n+1}} : v \in D_l^{(n)} \} \). If \( u \in D_l^{(n)} \), then
\[
u D_l^{(n)} = D_{l+u}^{(n)} \pmod{p^n}, \quad 0 \leq l, l' \leq p^n - 1.
\]
Proof. See [8] for the proofs of (i) and (ii).

Lemma 3.3. Assume \( \beta \in \mathbb{F}_d \) be any primitive \( p^{r+1} \)-th root of unity.
(i) If \( u, v \in D_l^{(n)} \) for some \( 0 \leq l' \leq p^n - 1 \), then \( D_l^{(n)}(\beta^{p^{r-n}u}) = D_l^{(n)}(\beta^{p^{r-n}v}) \).
(ii) If \( u \in D_l^{(n)} \), then \( D_l^{(n)}(\beta^{p^{r-n}v}) = D_{l+u}^{(n)} \pmod{p^n} \) with \( 0 \leq l, l' \leq p^n - 1 \).
(iii) For all \( u \in \mathbb{Z}_{p^{n+1}}^* \), \( p^n-1 \sum_{i=0}^{p^n-1} D_l^{(n)}(\beta^{p^{r-n}}) = 0 \).

The proofs of (i)-(iii) are similar to that of (ii)-(iv) of Lemma 2.2, thus we omit them here.

Lemma 3.4. Assume \( \beta \in \mathbb{F}_d \) be any primitive \( p^{r+1} \)-th root of unity. If \( dp^{r-1} \not\equiv 1 \pmod{p^2} \), then \( D_l^{(n)}(\beta^{p^{r-n}v}) \not\equiv 0 \), for all \( 0 \leq l \leq p^n - 1 \) and all \( v \in \mathbb{Z}_{p^{n+1}}^* \).

Proof. The proof of this claim is similar to that of Lemma 2.3 with following statement.
Denote by \( \lambda_n \) the multiplicative order of \( d \) modulo \( p^{n+1} \). Note here that \( \lambda_n \mid p^n(p-1) \). With the restriction that \( dp^{r-1} \not\equiv 1 \pmod{p^2} \), i.e., \( Q_p(d) \neq 0 \), we have \( Q_p(d) \neq 0 \) and \( \gcd(Q_p(d), p) = 1 \) for all integer \( n \geq 1 \) by [1, Corollary 5.7]. Thus, the definition of Euler quotients implies that
\[
d^{\lambda_n} \not\equiv 1 \pmod{p^{n+1}}
\]
and hence \( \lambda_n \mid p^n(p-1) \). So \( \lambda_n \geq p^n \) and \( d^{i} \not\equiv d^{j} \pmod{p^{n+1}} \) for \( 0 \leq i < j \leq p^n - 1 \). Suppose \( d \in D_{l_0}^{(n)} \) for some \( 1 \leq l_0 \leq p^n - 1 \) with \( \gcd(l_0, p) = 1 \). By (ii) of Lemma 3.2 we have \( d^{l'} \pmod{p^{n+1}} \in D_{l_0}^{(n)} \pmod{p^n} \) for all \( 0 \leq i \leq p^n - 1 \) and
\[
D_0^{(n)} \cup dD_0^{(n)} (= D_0^{(n)}) \cup \ldots \cup dp^{r-1}D_0^{(n)} = D_0^{(n)} \cup D_1^{(n)} \cup \ldots \cup D_{p^n-1}^{(n)} = \mathbb{Z}_{p^{n+1}}^*.
\]
Now we give a proof sketch for Theorem 3.1.

Proof of Theorem 3.1. We prove this theorem by the following two facts.
(i) If \( dp^{r-1} \not\equiv 1 \pmod{p^2} \), then \( H(\beta^v) \neq 0 \) for all \( u \in \mathbb{Z}_{p^{n+1}}^* \cup p\mathbb{Z}_{p^{r+1}}^* \cup \ldots \cup p^{r-1}\mathbb{Z}_{p^2}^* \).

For the simplicity, we denote
\[
M_n := p^{n-1} + \ldots + p + 1
\]
for all integers \( 1 \leq n \leq r \), thus
\[
M_r = p^n(p^{r-n-1} + \ldots + p + 1) + (p^{n-1} + \ldots + 1) = p^nM_{r-n} + M_n.
\]
If \( u \in p^{r-n}D^{(n)}_{l'} \) for \( 1 \leq n \leq r \) and \( 0 \leq l' \leq p^n - 1 \), write \( u = vp^{r-n} \) for some \( v \in D^{(n)}_{l'} \) and we derive

\[
H(\beta^u) = \sum_{j=1}^{d-1} j \sum_{l=jM_n+1}^{(j+1)M_n} D^{(r)}_l (\beta vp^{r-n})
= \sum_{j=1}^{d-1} j \sum_{l=jM_n+1}^{jM_n+\ell p^n M_{r-n}+\ell M_n} D^{(r)}_l (\beta vp^{r-n})
= \sum_{j=1}^{d-1} j \left( \sum_{l=jM_n+1}^{jM_n+\ell p^n M_{r-n}} D^{(r)}_l (\beta vp^{r-n}) + \sum_{l=jM_n+\ell p^n M_{r-n}+1}^{jM_n+\ell M_n} D^{(r)}_l (\beta vp^{r-n}) \right)
\]

Notice that \( \beta vp^{r-n} \in \mathbb{F}_d \) is a primitive \( p^{n+1} \)-th root of unity, by (a) of (i) and (ii) of Lemma 3.2, we have

\[
\sum_{l=jM_n+(k-1)p^n+1}^{jM_n+\ell p^n M_{r-n}} D^{(r)}_l (\beta vp^{r-n}) = \sum_{l=0}^{p^n-1} D^{(n)}_l (\beta vp^{r-n}) = 0
\]

for all \( 1 \leq k \leq \ell M_{r-n} \), which means that

\[
\sum_{l=jM_n+\ell p^n M_{r-n}+1}^{jM_n+\ell M_n} D^{(r)}_l (\beta vp^{r-n}) = \sum_{k=1}^{\ell M_{r-n}} \sum_{l=jM_n+(k-1)p^n+1}^{jM_n+\ell p^n M_{r-n}} D^{(r)}_l (\beta vp^{r-n}) = 0
\]

and

\[
\sum_{j=1}^{d-1} j \sum_{l=jM_n+\ell p^n M_{r-n}+1}^{jM_n+\ell M_n} D^{(r)}_l (\beta vp^{r-n}) = \sum_{j=1}^{d-1} j \sum_{l=jM_n+\ell M_n+1}^{jM_n+\ell p^n M_{r-n}+1} D^{(n)}_l (\beta vp^{r-n}).
\]

It follows that

\[
H(\beta^u) = H(\beta vp^{r-n}) = \sum_{j=1}^{d-1} j \sum_{l=jM_n+1}^{jM_n+\ell M_n} D^{(n)}_l (\beta vp^{r-n}).
\]

Thus, from (i) and (ii) of Lemma 3.3 and after a simple calculation we have

\[
H(\beta^u) = \sum_{j=0}^{d-1} (j-1) \sum_{l=jM_n+1}^{(j+1)M_n} D^{(n)}_l (\beta vp^{r-n}) - D^{(n)}_0 (\beta vp^{r-n}) + D^{(n)}_{\ell M_n} (\beta vp^{r-n})
\]

for \( a = bp^{r-n} \) with some \( b \in D^{(n)}_{\ell M_n} \).

Suppose that there is some \( a' \in p^{r-n}D^{(n)}_{k'} \) for some \( 0 \leq k' \leq p^n - 1 \) such that \( H(\beta^{a'}) = 0 \), the fact that \( D^{(n)}_k \cup D^{(n)}_{k+1} \cup \ldots \cup D^{(n)}_{k'+1} = \mathbb{Z}_p^{*} \) leads to \( H(\beta^u) = 0 \) holds for all \( u \in p^{r-n} \mathbb{Z}_p^{*} \). So we have \( H(\beta^{p^{r-n}}) = H(\beta^u) = 0 \), thus

\[
0 = -D^{(n)}_{\ell M_n} (\beta vp^{r-n}) = H(\beta^{p^{r-n}}) - H(\beta^u)
= \sum_{l=0}^{p^n-1} D^{(n)}_l (\beta vp^{r-n}) - D^{(n)}_{\ell M_n} (\beta vp^{r-n}).
\]

This contradicts Lemma 3.4. Therefore, for all \( u \in p^{r-n} \mathbb{Z}_p^{*} \) with \( 1 \leq n \leq r \), we always have \( H(\beta^u) \neq 0 \).

(viii) \( H(\beta^u) = 0 \), if \( u \in p^r \mathbb{Z}_p \).

The proof is similar to that of fact (ii) in the proof of Theorem 2.1, so we omit it.

Putting everything together, one can get the desired results.

\[\square\]
To illustrate the validity of Theorem 3.1, some examples of \(p^{r+1}\)-periodic \(d\)-ary sequences \((h_u)\) are given as follows:

| \(p\) | \(r\) | \(d\) | \(L((h_u))\) | \(L((h_u))\) satisfying |
|------|------|------|-------------|-----------------|
| 7    | 2    | 3    | 336         | \(p^3 - p\)     |
| 7    | 3    | 3    | 2394        | \(p^4 - p\)     |
| 11   | 2    | 5    | 1320        | \(p^3 - p\)     |
| 13   | 2    | 3    | 2184        | \(p^3 - p\)     |

4. Conclusion

For cryptographic purpose, one should construct pseudorandom sequences with high linear complexity according to the Berlekamp-Massey algorithm [15], which tells us that the complete sequences can be deduced from a knowledge of just \(2L\) terms from the sequences. So it is desired that the linear complexity should be at least half of the period. The linear complexity of the sequences in this article takes the values \(p^{r+1} - p\), which are larger than half of the period. Thus, it’s good enough from viewpoint of stream cipher.

It is natural to ask what will happen for the case of \(d^{p-1} \equiv 1 \pmod{p^2}\)? Remark that primes \(p\) such that \(a^{p-1} \equiv 1 \pmod{p^2}\) are called Wieferich primes with base \(a\) in [6, 13]. Historically, much computational effort has been devoted to finding solutions \(p\) and small fixed bases \(a\). Nevertheless, it has been known for more than a century [7] that for an arbitrarily chosen prime \(p\), infinitely many bases \(a\) exist for which \(a^{p-1} \equiv 1 \pmod{p^2}\) is satisfied. However, the known results show that such pairs \((a,p)\) with \(100 < a < 1000\) and \(10^4 < p < 10^{11}\) are rare. Thus, the result generalizes the earlier one derived from Fermat quotients in [2]. It is difficult to determine the exact value of the linear complexity, here we only present following results without proof.

**Theorem 4.1.** Let \((f_u)\) be the \(p^2\)-periodic \(d\)-ary sequence defined as in Eq. (2). If \(d^{p-1} \equiv 1 \pmod{p^2}\), then the linear complexity \(L((f_u))\) of \((f_u)\) satisfies

\[
L((f_u)) = p^2 - p - k(p - 1),
\]

for some \(1 \leq k \leq p - 1\).

**Theorem 4.2.** Let \((h_u)\) be the \(p^{r+1}\)-periodic \(d\)-ary sequence defined as in Eq. (5). If \(p\) is a Wieferich prime with base \(d\) and \(\mu(> 2)\) is the smallest integer with \(d^{p-1} \not\equiv 1 \pmod{p^{\mu}}\), then the linear complexity \(L((h_u))\) of \((h_u)\) satisfies

\[
L((h_u)) \geq p^{r+1} - p^{\delta+1} + \delta(p - 1),
\]

where \(\delta = \min\{r, \mu - 2\}\).

Acknowledgments

X.N.D. was partially supported by the National Natural Science Foundation of China under grants No. 61202395 and No. 61462077, the Program for New Century Excellent Talents in University (NCET-12-0620).

C.H.W. was partially supported by the National Natural Science Foundation of China under grant No. 61373140.
References

[1] T. Agoh, K. Dilcher and L. Skula, Fermat quotients for composite moduli, *J. Number Theory*, 66 (1997), 29–50.

[2] Z. Chen and X. Du, On the linear complexity of binary threshold sequences derived from Fermat quotients, *Des. Codes Cryptogr.*, 67 (2013), 317–323.

[3] Z. Chen, L. Hu and X. Du, Linear complexity of some binary sequences derived from Fermat quotients, *China Commun.*, 9 (2012), 105–108.

[4] Z. Chen, A. Ostafe and A. Winterhof, Structure of pseudorandom numbers derived from Fermat quotients, in *Proc. WAIFI 2010*, Springer-Verlag, Heidelberg, 2010, 73–85.

[5] Z. Chen and A. Winterhof, On the distribution of pseudorandom numbers and vectors derived from Euler-Fermat quotients, *Int. J. Number Theory*, 8 (2012), 631–641.

[6] R. Crandall, K. Dilcher and C. Pomerance, A search for Wieferich and Wilson primes, *Math. Comp.*, 66 (1997), 433–449.

[7] A. Cunningham, Period-lengths of circulates, *Messenger Math.*, 29 (1900), 145–179.

[8] X. Du, Z. Chen and L. Hu, Linear complexity of binary sequences derived from Euler quotients with prime-power modulus, *Inform. Proc. Letters*, 112 (2012), 604–609.

[9] X. Du, A. Klapper and Z. Chen, Linear complexity of pseudorandom sequences generated by Fermat quotients and their generalizations, *Inform. Proc. Letters*, 112 (2012), 233–237.

[10] R. Ernvall and T. Metsänkylä, On the p-divisibility of Fermat quotients, *Math. Comp.*, 66 (1997), 1353–1365.

[11] D. Gomez and A. Winterhof, Multiplicative character sums of Fermat quotients and pseudorandom sequences, *Period. Math. Hungar.*, 64 (2012), 161–168.

[12] A. Granville, Some conjectures related to Fermat’s Last Theorem, in *Number Theory*, Walter de Gruyter, Berlin, 1990, 177–192.

[13] W. Keller and J. Richstein, Prime solutions $p$ of $a^{p-1} \equiv 1$ (mod $p^2$) for prime bases $a$, *Math. Comput.*, 74 (2005), 927–936.

[14] R. Lidl and H. Niederreiter, *Finite Fields*, Addison-Wesley, Reading, MA, 1983.

[15] J. L. Massey, Shift register synthesis and BCH decoding, *IEEE Trans. Inform. Theory*, 15 (1969), 122–127.

[16] A. Ostafe and I. E. Shparlinski, Pseudorandomness and dynamics of Fermat quotients, *SIAM J. Discrete Math.*, 25 (2011), 50–71.

[17] A. Winterhof, Linear complexity and related complexity measures, in *Selected Topics in Information and Coding Theory*, World Scientific, 2010, 3–40.

[18] M. Sha, The arithmetic of Carmichael quotients, preprint, arXiv:1108.2579

[19] I. E. Shparlinski, Bounds of multiplicative character sums with Fermat quotients of primes, *Bull. Aust. Math. Soc.*, 83 (2011), 456–462.

[20] I. E. Shparlinski, Character sums with Fermat quotients, *Quart. J. Math.*, 62 (2011), 1031–1043.

[21] I. E. Shparlinski, Fermat quotients: Exponential sums, value set and primitive roots, *Bull. London Math. Soc.*, 43 (2011), 1228–1238.

[22] I. E. Shparlinski, On the value set of Fermat quotients, *Proc. Amer. Math. Soc.*, 140 (2012), 1199–1206.

Received for publication September 2014.

E-mail address: duxn@nwnu.edu.cn
E-mail address: wuchenhuan2008@126.com
E-mail address: yinLdxn@126.com