Linear complexity of binary sequences derived from Euler quotients with prime-power modulus

Xiaoni Du\textsuperscript{a,b}, Zhixiong Chen\textsuperscript{c,d,*}, Lei Hu\textsuperscript{d}

\textsuperscript{a} College of Mathematics and Information Science, Northwest Normal University, Lanzhou, Gansu 730070, PR China
\textsuperscript{b} State Key Lab. of Integrated Service Networks, Xidian University, Xi’an, Shaanxi 710071, PR China
\textsuperscript{c} Department of Mathematics, Putian University, Putian, Fujian 351100, PR China
\textsuperscript{d} State Key Laboratory of Information Security, Graduate School of Chinese Academy of Sciences, Beijing 100049, PR China

Abstract

We extend the definition of binary threshold sequences from Fermat quotients to Euler quotients modulo $p^r$ with odd prime $p$ and $r \geq 1$. Under the condition of $2^p - 1 \not\equiv 1 \pmod{p^2}$, we present exact values of the linear complexity by defining cyclotomic classes modulo $p^n$ for all $1 \leq n \leq r$. The linear complexity is very close to the period and is of desired value for cryptographic purpose. We also present a lower bound on the linear complexity for the case of $2^p - 1 \equiv 1 \pmod{p^2}$.

© 2012 Elsevier B.V. All rights reserved.

1. Introduction

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

$Q_{p^r}(u) \equiv \frac{u^{\phi(p^r)} - 1}{p^r}$ (mod $p^r$),

$0 \leq Q_{p^r}(u) \leq p^r - 1,$

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

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

See, e.g., [1,5,14] for details.

If $r = 1$, $Q_p(u)$ is just the Fermat quotient studied in [7, 9,13,15–18] and references therein. More recently, Fermat quotients are studied from the viewpoint of cryptography, see [2–4,6,8,13].

Motivated by the previous work [2–4], we define a family of binary sequences $(e_u)$ by using the Euler quotient $Q_{p^r}(u)$ by

$e_u = \begin{cases} 
0, & \text{if } 0 \leq Q_{p^r}(u)/p^r < \frac{1}{2}, \\
1, & \text{if } \frac{1}{2} \leq Q_{p^r}(u)/p^r < 1.
\end{cases}$ \quad (1)

We note that $(e_u)$ is $p^{r+1}$-periodic since $Q_{p^r}(u)$ is a $p^{r+1}$-periodic sequence modulo $p^r$ by the fact

$Q_{p^r}(u + kp^r) \equiv Q_{p^r}(u) - kp^{r-1}u^{-1} \pmod{p^r}$ \quad (2)

for any integer $k$ and $u$ with $\gcd(u, p) = 1$. In fact, for such $u$, we have

$Q_{p^r}(u + kp^r) \equiv \frac{(u + kp^r)^{\phi(p^r)} - 1}{p^r}$.
For $r = 1$, linear complexity of $(e_u)$ defined in (1) was investigated in [2]. 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 $(s_u)$ over the binary field $F_2$ is the least order $L$ of a linear recurrence relation over $F_2$

$s_{u+L} = c_{l-1}s_{u+L-1} + \cdots + c_1s_{u+1} + c_0s_u$ for $u \geq 0$

which is satisfied by $(s_u)$ and where $c_0 = 1, c_1, \ldots, c_{l-1} \in F_2$. The polynomial

$M(x) = x^L + c_{l-1}x^{L-1} + \cdots + c_0 \in F_2[x]$

is called the minimal polynomial of $(s_u)$. The generating polynomial of $(s_u)$ is defined by

$s(x) = s_0 + s_1x + s_2x^2 + \cdots + s_{T-1}x^{T-1} \in F_2[x].$

It is easy to see that

$M(x) = (x^T - 1)/\gcd(x^T - 1, s(x)).$

hence

$L((s_u)) = T - \deg(\gcd(x^T - 1, s(x))).$

(3)

which is the degree of the minimal polynomial, see [11,19] for a more detailed exposition.

We will extend the result of [2] to show the following theorem.

**Theorem 1.** Let $(e_u)$ be the $p^{t+1}$-periodic binary sequence defined as in Eq. (1). If $2p^{t+1} \equiv 1 \pmod{p^2}$, then the linear complexity $L((e_u))$ of $(e_u)$ satisfies

$L((e_u)) = \begin{cases} p^{t+1} - 1 - p, & \text{if } p \equiv 1 \pmod{4}, \\ p^{t+1} - 1 - p, & \text{if } p \equiv 3 \pmod{4} \text{ and } r \text{ is even}, \\ p^{t+1} - 1, & \text{if } p \equiv 3 \pmod{4} \text{ and } r \text{ is odd}. \end{cases}$

2. Auxiliary lemmas

In order to prove the theorem, we will define a partition of the residue class ring modulo $p^{n+1}$ with respect to the Euler quotient $Q_{p^s}(u)$ for $1 \leq n \leq r$. We denote by $Z_{p^n} = \{0, 1, \ldots, p^n - 1\}$ the residue class ring modulo $p^n$ and by $Z_{p^n}^*$ the unit group of $Z_{p^n}$ for $n \geq 1$. Let

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

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

$e_u = \begin{cases} 0, & \text{if } u \in D_0^{(r)} \cup \cdots \cup D_{(p^n-1)/2}^{(r)} \cup pZ_{p^r}, \\ 1, & \text{if } u \in D_{(p^n-1)/2}^{(r)} \cup \cdots \cup D_{p^n-1}^{(r)}, \end{cases}$

$0 \leq u \leq p^{n+1} - 1,$

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

**Lemma 1.** For all $n \geq 1$, let $uD_l^{(n)} = \{uv \pmod{p^{n+1}}: v \in D_l^{(n)}\}$. If $u \in D_1^{(n)}$, then we have

$uD_l^{(n)} = D_{l+l'}^{(n)} \pmod{p^r},$

where $0 \leq l, l' \leq p^n - 1$.

**Proof.** It is easy to get the desired result from the fact that

$Q_{p^n}(uv) \equiv Q_{p^n}(u) + Q_{p^n}(v) \pmod{p^r}$

for integers $u, v$ with $\gcd(uv, p) = 1$, see [1].

**Lemma 2.** (i) For $n' \geq n \geq 1$ and $0 \leq l' \leq p^n - 1$, we have

$\{u \pmod{p^{n+1}}: u \in D_{l'}^{(n)}\} = D_{l'}^{(n)} \pmod{p^r}.$

(ii) For $n \geq 1$ and $0 \leq l \leq p^n - 1$, we have

$\{u \pmod{p^n}: u \in D_l^{(n)}\} = \{1, 2, \ldots, p^n - 1\}.$

**Proof.** For all integers $n \geq 1$ by [1, Proposition 4.4 and Corollary 4.4], $Q_{p^n}(u)$ induces a group epimorphism

$Q_{p^n} : Z_{p^{n+1}}^* \to (Z_{p^n}, +)$

with kernel $D_0^{(n)}$ of order $p - 1$. So each $D_l^{(n)}$ has $p - 1$ elements for $1 \leq l < p^n$.

(i) It is sufficient to show the case of $n' = n + 1$, then the claim follows by induction.

For any $u \in D_l^{(n+1)}$, by [1, Proposition 4.1] we have

$Q_{p^n}(u) \equiv Q_{p^{n+1}}(u) \equiv l' \pmod{p^r},$

which indicates that $u \pmod{p^{n+1}}$ belongs to $D_{l'}^{(n+1)}$. Since $p^{n+1}$ is a period of $Q_{p^n}(u)$, so we get

$\{u \pmod{p^{n+1}}: u \in D_{l'}^{(n+1)}\} \subseteq D_{l'}^{(n)} \pmod{p^r}.$

Then we show the cardinality of $(u \pmod{p^{n+1}}: u \in D_{l'}^{(n+1)})$ is $p - 1$, equal to that of $D_{l'}^{(n)} \pmod{p^r}$. In fact, if $u = u' \pmod{p^{n+1}}$ for $u, u' \in D_{l'}^{(n+1)}$, we suppose $u = u' + k_0p^{n+1}$ for some $0 \leq k_0 < p$. We have

$l' \equiv Q_{p^{n+1}}(u') \equiv Q_{p^{n+1}}(u' + k_0p^{n+1}) \equiv Q_{p^{n+1}}(u') - k_0u^{-1}p^n \pmod{p^{n+1}},$

which indicates that $k_0 = 0$ and $u = u'$. We prove the first result.
Lemma 3. For all \( n \geq 1 \), let \( \theta_n \in \mathbb{F}_2 \) be any primitive \( p^{n+1} \)-th root of unity. Then for all \( u \in \mathbb{Z}_{p^{n+1}}^* \), we have

\[
\sum_{l=0}^{p^n-1} D_l^{(n)}(\theta_n^u) = 0.
\]

Proof. It is easy to check that for all \( u \in \mathbb{Z}_{p^{n+1}}^* \)

\[
\sum_{i \in \mathbb{Z}_{p^{n+1}}} \theta_n^{u_i} = \frac{1 - \theta_n^{p^{n+1}}}{1 - \theta_n} = 0
\]

and

\[
\sum_{i \in \mathbb{Z}_{p^n}} \theta_n^{u_i} = \frac{1 - \theta_n^{p^n}}{1 - \theta_n^{p^n}} = 0.
\]

So we get that

\[
\sum_{l=0}^{p^n-1} D_l^{(n)}(\theta_n^u) = \sum_{i \in \mathbb{Z}_{p^{n+1}}} \theta_n^{u_i} = \sum_{i \in \mathbb{Z}_{p^{n+1}}} \theta_n^{u_i} - \sum_{i \in \mathbb{Z}_{p^n}} \theta_n^{u_i} = 0.
\]

For convenience, we denote

\[
\Delta_{\ell}^{(n)}(x) = \sum_{l=\frac{p^n+1}{2}}^{p^n+\ell} D_l^{(n)}(x) \in \mathbb{F}_2[x]
\]

for \( 1 \leq n \leq r \) and \( 0 \leq \ell \leq p^n - 1 \). Clearly \( E(x) = \Delta_0^{(r)}(x) \).

Lemma 4. For all \( n \geq 1 \), let \( \theta_n \in \mathbb{F}_2 \) be any primitive \( p^{n+1} \)-th root of unity. If \( u \in \mathbb{D}_{\ell}^{(n)} \), then we have

\[
\Delta_{\ell}^{(n)}(\theta_n^u) = \Delta_{\ell+\ell'}^{(n)}(\theta_n^u),
\]

where \( 0 \leq \ell, \ell' \leq p^n - 1 \).

Proof. By Lemma 1 and the definition of \( D_l^{(n)}(x) \), we know that

\[
D_{l+\ell'}^{(n)}(\theta_n^u) = \sum_{l=\frac{p^n+1}{2}}^{p^n+\ell+\ell'} D_l^{(n)}(\theta_n^u) = \sum_{l=\frac{p^n+1}{2}}^{p^n+\ell} D_l^{(n)}(\theta_n^u) + \sum_{l=\frac{p^n+1}{2}}^{\ell'-1} D_l^{(n)}(\theta_n^u)
\]

for \( n \geq 1 \) and \( \ell, \ell' \leq p^n - 1 \). Then

\[
\Delta_{\ell+\ell'}^{(n)}(\theta_n^u) = \sum_{l=\frac{p^n+1}{2}}^{p^n+\ell+\ell'} D_l^{(n)}(\theta_n^u) = \sum_{l=\frac{p^n+1}{2}}^{p^n+\ell} D_l^{(n)}(\theta_n^u) + \sum_{l=\frac{p^n+1}{2}}^{\ell'-1} D_l^{(n)}(\theta_n^u) = \Delta_{\ell}^{(n)}(\theta_n^u).
\]

Lemma 5. Let \( \beta \in \mathbb{F}_2 \) be a primitive \( p^{r+1} \)-th root of unity. We have

\[
E(\beta^u) = \begin{cases} 0, & \text{if } u = 0, \\ \frac{p^r-1}{2}, & \text{if } u \equiv p^{r} \beta \pmod{p^r}, \\ \Delta_{\ell}^{(n)}(\beta^{p^r-\ell}), & \text{if } u \equiv \beta^{p^r-\ell} D_{\ell}^{(n)}, \\ 1 \leq n \leq r, 0 \leq \ell \leq p^n - 1. & \end{cases}
\]

Proof. (i) If \( u = 0 \), since each \( D_l^{(r)} \) has \( p - 1 \) elements, we have

\[
E(\beta^0) = E(1) = \sum_{l=\frac{p^r+1}{2}}^{p^r-1} \sum_{j \in D_l^{(r)}} 1 = \frac{(p^r-1)(p-1)}{2} \equiv 0 \pmod{2}.
\]

(ii) If \( u \equiv \beta^v \pmod{p^r} \), write \( u = v p^r \) for some \( v \in \mathbb{Z}_p^* \) and we derive

\[
E(\beta^u) = \sum_{l=\frac{p^r+1}{2}}^{p^r-1} \sum_{j \in D_l^{(r)}} \beta^v p^r = \sum_{l=\frac{p^r+1}{2}}^{p^r-1} \sum_{j \in D_l^{(r)}} (\beta^v)^j = \sum_{l=\frac{p^r+1}{2}}^{p^r-1} (\beta^v + \beta^v p^r + \ldots + \beta^{p^r-1} p^r) = \sum_{l=\frac{p^r+1}{2}}^{p^r-1} \frac{\beta^v (1 - \beta^{p-1} p^r)}{1 - \beta^v}.
\]
Lemma 6. For all \( \beta \neq 0 \) and \( \delta \), if \( u \in p^{r-n}D_{\ell}^{(n)} \) for \( 1 \leq n \leq r \) and \( 0 \leq \ell \leq p^n - 1 \), write \( u = vp^n - r \) for some \( v \in D_{\ell}^{(n)} \) and we derive
\[
E(\beta^u) = \sum_{l=\ell}^{p^n-1} \sum_{j \in D_{\ell}^{(n)}} (\beta vp^n - r)^j
\]
\[
= \sum_{k=0}^{p^n-r-1} \sum_{l=\ell}^{p^n-1} \sum_{j \in D_{\ell}^{(n)}} (\beta vp^n - r)^j
\]
\[
+ \sum_{l=\ell}^{p^n-1} \sum_{j \in D_{\ell}^{(n)}} (\beta vp^n - r)^j
\]
Notice that \( \beta vp^n - r \in F_2 \) is a \( p^{r+1} \)-th primitive root of unity, by Lemmas 2(iii) and 3 we have
\[
\sum_{l=\ell}^{p^n-1} \sum_{j \in D_{\ell}^{(n)}} (\beta vp^n - r)^j = \sum_{l=0}^{p^n-r-1} \sum_{j \in D_{\ell}^{(n)}} (\beta vp^n - r)^j = 0
\]
for all \( k \geq 1 \), and
\[
\sum_{l=\ell}^{p^n-1} \sum_{j \in D_{\ell}^{(n)}} (\beta vp^n - r)^j = \sum_{l=0}^{p^n-r-1} \sum_{j \in D_{\ell}^{(n)}} (\beta vp^n - r)^j = \Delta_\ell^{(n)}(\beta vp^n - r).
\]
Thus by Lemma 4, we have
\[
E(\beta^u) = \Delta_\ell^{(n)}(\beta vp^n - r) = \Delta_\ell^{(n)}(\beta vp^n - r).
\]

Lemma 6. Let \( \beta \in F_p \) be a primitive \( p^{r+1} \)-th root of unity. If \( 2^{p-1} \equiv 1 \) (mod \( p^2 \)), we have \( E(\beta^u) \neq 0 \) for all \( u \in Z_{p^{r+1}} \cup pZ_{p^{r+1}} \cup \cdots \cup p^{r-2}Z_{p^{r+1}} \).  

Proof. Let \( u \in p^{r-n}Z_{p^{r+1}} \) for \( 1 \leq n \leq r \) and \( 0 \leq \ell \leq p^n - 1 \). By Lemma 5 we only need to prove
\[
\Delta_\ell^{(n)}(\beta vp^n - r) \neq 0.
\]
Suppose that there exist \( 1 \leq n_0 \leq r \) and \( 0 \leq \ell_0 \leq p^{n_0} - 1 \) such that
\[
\Delta_{\ell_0}^{(n_0)}(\beta vp^{n_0} - r) = 0.
\]
Using the restriction that \( 2^{p-1} \neq 1 \) (mod \( p^2 \)), i.e., \( Q_p(2) \neq 0 \), we have \( Q_p^{(n_0)}(2) \neq 0 \) and \( \gcd(Q_p^{(n_0)}(2), p) = 1 \) by [1, Corollary 5.7]. So we suppose \( 2 \in D_{\ell_0}^{(n_0)} \) for some \( 1 \leq \ell_0 \leq p^{n_0} - 1 \) with \( \gcd(\ell, p) = 1 \). By Lemma 1 we have \( 2^{l_0} \) (mod \( p^{n+1} \)) \( \in D_{\ell_0}^{(n)} \) (mod \( p^n \)) for all \( 0 \leq j \leq p^n - 1 \). Then, by Lemma 4 we derive
\[
0 = (\Delta_{\ell_0}^{(n)}(\beta vp^{n_0} - r))^{2^j} = \Delta_{\ell_0}^{(n)}(\beta^{2^j}p^{n_0} - r)
\]
\[
= \Delta_{\ell_0}^{(n)}(\beta^2p^{n_0} - r)
\]
for all \( 0 \leq j \leq p^n - 1 \). On the other hand, according to the definition of Euler quotients, \( Q_{p^{n_0}}(2) \neq 0 \) implies that
\[
2^j(p^{n_0}) \neq 1 \ (\text{mod} \ p^{n_0}+1)
\]
and hence \( 2^j \neq 2^l \ (\text{mod} \ p^{n_0}+1) \) for \( 0 \leq i < j \leq p^n - 1 \). Thus Eq. (5) implies
\[
\Delta_{\ell_0}^{(n)}(\beta^{2^j}p^{n_0} - r) = 0
\]
for all \( 0 \leq \ell \leq p^{n_0} - 1 \). Furthermore, we have
\[
\Delta_{\ell_0}^{(n)}(\beta^{2^j}p^{n_0} - r) = 0
\]
for all \( 0 \leq \ell \leq p^{n_0} - 1 \) and \( v \in Z_{p^{n_0}+1} \) by Lemma 4 again.

Therefore, we get that for all \( j = 0, 1, \ldots, p^n - 1 \) and all \( v \in Z_{p^{n_0}+1} \),
\[
D_{\ell_0}^{(n)}(\beta^{2^j}p^{n_0} - r) \neq 0
\]
by Lemma 3. That is, each polynomial \( D_{\ell_0}^{(n)}(x) \) has at least \( p^n(p-1) \) many roots for \( j = 0, 1, \ldots, p^n - 1 \). Using a similar proof of [2, Lemma 4], we deduce that there exists at least one \( D_{\ell_0}^{(n)}(x) \) such that \( \deg(D_{\ell_0}^{(n)}(x)) < p^n(p-1) \), which is a contradiction to the fact that the polynomial \( D_{\ell_0}^{(n)}(x) \) has \( p^n(p-1) \) different roots. So we get the desired result. 

3. Proof of the main theorem and conclusions

Proof of Theorem 1. If \( p \equiv 1 \) (mod \( 4 \)), we have \( E(\beta^u) = 0 \) if and only if \( u \in p^jZ_p \) by Lemmas 5 and 6. The number of the common roots of \( E(x) \) and \( x^{2^{p-1}} - 1 \) is \( p \), so the linear complexity of \( (e_u) \) is \( p^{r+1} - p \) by Eq. (3). Similarly, if \( p \equiv 3 \) (mod \( 4 \)), we have \( E(\beta^u) = 0 \) if and only if either \( r \) is odd and \( u = 0 \) or \( r \) is even and \( u \in p^jZ_p \), which implies the linear complexity of \( (e_u) \).

We have determined the linear complexity of a family of binary threshold sequences defined by using the Euler quotients modulo an odd prime-power \( p^2 \), where \( p \) satisfies that \( 2^{p-1} \neq 1 \) (mod \( p^2 \)). The result generalizes the earlier one derived from Fermat quotients in [2].

For cryptographic purpose, one should construct pseudorandom sequences with high linear complexity according to the Berlekamp–Massey algorithm [12], which tells us that the complete sequences can be deduced from a
knowledge of just 2L (here L is the linear complexity) consecutive terms from the sequences. So it is desired that the linear complexity should be at least half of the period. The linear complexity in this article takes the values \( p^{r+1} - p \) or \( p^{r+1} - 1 \), which are larger than half of the period.

From the proof of Theorem 1, it is easy to see that the minimal polynomial \( M(x) \) of \( (e_u) \) satisfies

\[
M(x) = \begin{cases} 
(x^{p+1} - 1)/(x^p - 1), & \text{if } p \equiv 1 \pmod{4}, \\
(x^{p+1} - 1)/(x - 1), & \text{if } p \equiv 3 \pmod{4}.
\end{cases}
\]

So by Lemma 5, there are \( k_0(p - 1) \) many \( u \in \mathbb{F}_{p^n}^* \) satisfying \( E(\beta^u) \neq 0 \), where \( 1 \leq k_0 \leq p^n - 1 \). However, for each \( n \): \( \delta < n \leq r \) if \( \delta < r \), we have \( E(\beta^u) \neq 0 \) for all \( u \in \mathbb{F}_{p^n}^* \).

Putting everything together, we see that the linear complexity \( L((e_u)) \) is of the form

\[
L((e_u)) = \sum_{n=1}^{\delta} k_n(p - 1) + \sum_{n=4+1}^r \varphi(p^{n+1})
\]

where \( 1 \leq k_n \leq p^n - 1 \) and \( n \leq \delta \). Each \( k_n = 1 \) leads to the lower bound. \( \square \)

Acknowledgements

The authors wish to thank the anonymous referee for his valuable comments, in particular for pointing out the issue of lower bounds on the linear complexity for the case of Wieferich primes. The authors also wish to thank Prof. Igor E. Shparlinski for his helpful comments.

X.N.D. was partially supported by the National Natural Science Foundation of China under grant 61003094, the Funds of the Education Department of Gansu Province under grant 10019-09. Part of the work was written during a pleasant visit of X.N.D. to Lexington. She wishes to thank the University of Kentucky for hospitality and support.

Z.X.C. was partially supported by the National Natural Science Foundation of China under grant No. 61170246, the Program for New Century Excellent Talents in Fujian Province University of China under grant No. J2K2010047 and the Open Funds of State Key Laboratory of Information Security (Chinese Academy of Sciences) under grant No. 01-01-1.

L.H. was partially supported by the National Natural Science Foundation of China under Grant Nos. 61070172 and 10990011.

References


