On the $k$-error linear complexity of binary sequences derived from polynomial quotients

CHEN ZhiXiong$^1$, NIU ZhiHua$^2$ & WU ChenHuang$^1$

$^1$School of Mathematics, Putian University, Putian 351100, China; 
$^2$School of Computer Engineering and Science, Shanghai University, Shanghai 200444, China

Received August 1, 2014; accepted October 9, 2014; published online June 26, 2015

Abstract The $k$-error linear complexity is an important cryptographic measure of pseudorandom sequences in stream ciphers. In this paper, we investigate the $k$-error linear complexity of $p^2$-periodic binary sequences defined from the polynomial quotients modulo $p$, which are the generalizations of the well-studied Fermat quotients. Indeed, first we determine exact values of the $k$-error linear complexity over the finite field $F_2$ for these binary sequences under the assumption of 2 being a primitive root modulo $p^2$, and then we determine their $k$-error linear complexity over the finite field $F_p$. Theoretical results obtained indicate that such sequences possess ‘good’ error linear complexity.

Keywords cryptography, Fermat quotients, polynomial quotients, binary sequences, linear complexity, $k$-error linear complexity

Citation Chen Z X, Niu Z H, Wu C H. On the $k$-error linear complexity of binary sequences derived from polynomial quotients. Sci China Inf Sci, 2015, 58: 092107(15), doi: 10.1007/s11432-014-5220-7

1 Introduction

For an odd prime $p$ and integers $u \geq 0$ with $\gcd(u,p) = 1$, the Fermat quotient $q_p(u)$ is defined as the unique integer

$$q_p(u) \equiv \frac{u^{p-1} - 1}{p} \mod p \text{ with } 0 \leq q_p(u) \leq p - 1,$$

and

$$q_p(lp) = 0, \quad l \in \mathbb{Z}.$$  

An equivalent definition of the Fermat quotient is given below

$$q_p(u) \equiv \frac{u^{p-1} - u^{p^{p-1}}}{p} \mod p, \quad u \geq 0. \quad (1)$$

For any fixed positive integer $w$, by the fact that $(u^w)^p \equiv u^w \mod p$, $u \geq 0$ from the Fermat Little Theorem, Chen and Winterhof [1] extended (1) to define

$$q_{p,w}(u) \equiv \frac{u^w - u^{wp}}{p} \mod p \text{ with } 0 \leq q_{p,w}(u) \leq p - 1, \quad u \geq 0, \quad (2)$$

* Corresponding author (email: ptczx@126.com)
which is called a polynomial quotient. In fact \( q_{p,w}(u) = q_p(u) \). It is easy to see that

\[
q_{p,w}(u + lp) = q_{p,w}(u) + uw^{w-1} \pmod{p}
\]

(3)

if \( \gcd(u, p) = 1 \), and

\[
q_{p,w}(lp) = \begin{cases} 
0, & \text{if } w > 1, \\
l, & \text{if } w = 1, 
\end{cases} \quad l = 0, \ldots, p - 1.
\]

(4)

Many number theoretic and cryptographic questions as well as measures of pseudorandomness have been studied for Fermat quotients and their generalizations [1–21].

In this paper, we still concentrate on certain binary sequences defined from the polynomial quotients (of course including the Fermat quotients) in the references. The first one is the binary threshold sequence \( (e_u) \) studied in [6–8, 12, 22, 23] by defining

\[
e_u = \begin{cases} 
0, & \text{if } 0 \leq q_{p,w}(u)/p < \frac{1}{2}, \\
1, & \text{if } \frac{1}{2} \leq q_{p,w}(u)/p < 1, 
\end{cases} \quad u \geq 0.
\]

(5)

The second one, by combining \( q_{p,w}(u) \) with the Legendre symbol \( \left( \frac{u}{p} \right) \), is defined in [12,14,22,23] by

\[
f_u = \begin{cases} 
0, & \text{if } \left( \frac{q_{p,w}(u)}{p} \right) = 1 \text{ or } q_{p,w}(u) = 0, \\
1, & \text{otherwise}, 
\end{cases} \quad u \geq 0.
\]

(6)

In fact, in [12,14], \( \chi \), a fixed multiplicative character modulo \( p \) of order \( m > 1 \), is applied to defining \( m \)-ary sequences \( (f_u) \) of discrete logarithms modulo a divisor \( m \) of \( p - 1 \) by

\[
\exp(2\pi i f_u/m) = \chi(q_{p,w}(u)), \quad 0 \leq f_u < m,
\]

if \( q_{p,w}(u) \not\equiv 0 \pmod{p} \) and \( f_u = 0 \) otherwise. When \( m = 2 \), we have \( f_u = e_u \) for all \( u \geq 0 \). We note that both \( (e_u) \) and \( (f_u) \) are \( p^2 \)-periodic by (3).

The authors of [8,14] investigated measures of pseudorandomness as well as linear complexity profile of \( (e_u) \) and \( (f_u) \) (of course including \( (f_u) \)) via certain character sums over Fermat quotients. The authors of [12, 23] determined the linear complexity (see below for the definition) of \( (e_u) \) and \( (f_u) \) if 2 is a primitive root modulo \( p^2 \), and later the authors of [6,7,22] extended to a more general setting of \( 2^{\varphi - 1} \equiv 1 \pmod{p^2} \) when \( w \in \{p - 1, (p - 1)/2\} \). The author of [22] also determined the trace representations of \( (e_u) \) and \( (f_u) \). In this paper, our main aim is to study the \( k \)-error linear complexity (see below for the definition) for \( (e_u) \) and \( (f_u) \). All results indicate that such sequences have desirable cryptographic features.

For our purpose, we need to describe \( (e_u) \) and \( (f_u) \) in an equivalent way. From (3), \( q_{p,w}(-) \) induces a surjective map from \( \mathbb{Z}_p^* \) (the group of invertible elements modulo \( p^2 \)) to \( \mathbb{Z}_p \) (the additive group of numbers modulo \( p \)). For each fixed \( 1 \leq w < p \), we define

\[
D_l = \{ u : 0 \leq u < p^2, \gcd(u, p) = 1, \ q_{p,w}(u) = l \},
\]

for \( l = 0, 1, \ldots, p - 1 \). Each \( D_l \) has the cardinality \( |D_l| = p - 1 \) by (3). Here and hereafter, we use \( |S| \) to denote the cardinality of a set \( S \). Let \( P = \{ lp : 0 \leq l < p \} \), for \( w \geq 2 \) one can define \( (e_u) \) and \( (f_u) \) equivalently by

\[
e_u = \begin{cases} 
0, & \text{if } u \mod p^2 \in D_0 \cup \ldots \cup D_{(p-1)/2} \cup P, \\
1, & \text{if } u \mod p^2 \in D_{(p+1)/2} \cup \ldots \cup D_{p-1}, 
\end{cases}
\]

and

\[
f_u = \begin{cases} 
0, & \text{if } u \mod p^2 \in \cup_{l \in Q} D_l \cup D_0 \cup P, \\
1, & \text{if } u \mod p^2 \in \cup_{l \in N} D_l, 
\end{cases}
\]

respectively, where \( Q \) is the set of quadratic residues modulo \( p \) and \( N \) is the set of quadratic non-residues modulo \( p \). For \( w = 1 \), it is easy to define \( (e_u) \) and \( (f_u) \) similarly by only re-dividing the set \( P \).