SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

March 2016, Vol. 59 032106:1–032106:12
doi: 10.1007/s11432-015-5305-y

Linear complexity problems of level sequences of Euler quotients and their related binary sequences

Zhihua NIU[1]*, Zhixiong CHEN[2] & Xiaoni DU[3]

[1]*School of Computer Engineering and Science, Shanghai University, Shanghai* 200444*, China;*
[2]*School of Mathematics, Putian University, Putian* 351100*, China;*
[3]*College of Mathematics and Information Science, Northwest Normal University, Lanzhou* 730070*, China*

Received October 22, 2014; accepted January 8, 2015; published online July 13, 2015

Abstract The Euler quotient modulo an odd-prime power p^r $(r > 1)$ can be uniquely decomposed as a p-adic number of the form $(u^{(p-1)p^{r-1}} - 1)/p^r \equiv a_0(u) + a_1(u)p + \cdots + a_{r-1}(u)p^{r-1} \pmod{p^r}$, $\gcd(u, p) = 1$, where $0 \leqslant a_j(u) < p$ for $0 \leqslant j \leqslant r-1$ and we set all $a_j(u) = 0$ if $\gcd(u, p) > 1$. We firstly study certain arithmetic properties of the level sequences $(a_j(u))_{u \geqslant 0}$ over $\mathbb{F}_p$ via introducing a new quotient. Then we determine the exact values of linear complexity of $(a_j(u))_{u \geqslant 0}$ and values of k-error linear complexity for binary sequences defined by $(a_j(u))_{u \geqslant 0}$.

Keywords cryptography, Euler quotients, Fermat quotients, pseudorandom sequences, binary sequences, linear complexity, k-error linear complexity

Citation Niu Z H, Chen Z X, Du X N. Linear complexity problems of level sequences of Euler quotients and their related binary sequences. Sci China Inf Sci, 2016, 59(3): 032106, doi: 10.1007/s11432-015-5305-y

1 Introduction

Let p be an odd prime and r be a positive integer. For all integers u with $\gcd(u, p) = 1$, by the Euler Theorem we have

$$u^{\varphi(p^r)} \equiv 1 \pmod{p^r},$$

where $\varphi(-)$ is the Euler Totient function. Hence we define $Q_r(u)$ modulo p^r by

$$Q_r(u) \equiv \frac{u^{\varphi(p^r)} - 1}{p^r} \pmod{p^r},\ 0 \leqslant Q_r(u) < p^r,\ \text{if } \gcd(u, p) = 1, \tag{1}$$

which is called the *Euler quotient* in [1]. In fact, if we write

$$u^{\varphi(p^r)} = 1 + a_1 p^r + a_2 p^{2r} + \cdots \in \mathbb{Z},\ 0 \leqslant a_i < p^r \text{ for } i \geqslant 1, \tag{2}$$

we have $Q_r(u) = a_1$. For convenience, we set

$$Q_r(lp) = 0, \quad l \in \mathbb{Z}. \tag{3}$$

* Corresponding author (email: zhniu@staff.shu.edu.cn)

If $r = 1$, $Q_1(u)$ is also called the *Fermat quotient*. A more general notion, called the *Carmichael Quotient*, is studied in [2]. Many number theoretic questions have been studied for these quotients and their generalizations [1–16].

Let $\mathbb{Z}_{p^r}$ be the integer residue ring modulo p^r. Any element $a \in \mathbb{Z}_{p^r}$ has a unique p-adic decomposition as $a = a_0 + a_1 p + \cdots + a_{r-1}p^{r-1}$, where $a_i \in \{0, 1, \ldots, p-1\}$. Hence for a sequence $(s(u))_{u\geqslant 0}$ over $\mathbb{Z}_{p^r}$, it has a unique p-adic decomposition as

$$s(u) = s_0(u) + s_1(u)p + \cdots + s_{r-1}(u)p^{r-1}, \quad u \geqslant 0,$$

where $(s_i(u))_{u\geqslant 0}$ is a sequence over $\{0, 1, \ldots, p-1\}$. The sequence $(s_i(u))_{u\geqslant 0}$ is called the *ith level sequence* of $(s(u))_{u\geqslant 0}$, and $(s_{r-1}(u))_{u\geqslant 0}$ the *highest-level sequence* of $(s(u))_{u\geqslant 0}$. They can be naturally considered as the sequences over the finite field $\mathbb{F}_p$. Fan and Qi (partly with coauthors) extensively investigated the level sequences of linear recurring sequences over $\mathbb{Z}_{p^r}$ (or more generally $\mathbb{Z}_M$, where $M > 1$ is an arbitrary number), see [17–23] and references therein. Certain $(s(u))_{u\geqslant 0}$ over $\mathbb{Z}_{p^r}$ is relevant to FCSR sequences [24].

On the other hand, Fermat quotients, Euler quotients and Carmichael Quotients have been studied recently from the viewpoint of cryptography, see [5, 10, 11, 25–34]. More exactly, the authors of [11] studied the linear complexity profile of the Fermat quotient sequence $(Q_1(u))_{u\geqslant 0}$. As we know, this is the first work to consider the cryptographic feature of Fermat quotients. The authors of [5, 10] used Fermat quotients and Euler quotients to define pseudorandom sequences. The first one is the binary threshold sequence $(e(u))_{u\geqslant 0}$ defined by

$$e(u) = \begin{cases} 0, & \text{if } 0 \leqslant Q_r(u)/p^r < \frac{1}{2}, \\ 1, & \text{if } \frac{1}{2} \leqslant Q_r(u)/p^r < 1, \end{cases} \quad u \geqslant 0. \tag{4}$$

The second one, by combining $Q_r(u)$ with χ, which is a fixed multiplicative character modulo p^r of order $m > 1$, is the m-ary sequences $(\widetilde{e}(u))_{u\geqslant 0}$ defined by

$$\exp(2\pi i\widetilde{e}(u)/m) = \chi(Q_r(u)),\ 0 \leqslant \widetilde{e}(u) < m \text{ if } \gcd(Q_r(u), p) = 1 \tag{5}$$

and $\widetilde{e}(u) = 0$ otherwise. Most recent studies are concentrated in the case of $r = 1$: the authors of [5,10] investigated measures of pseudorandomness as well as linear complexity profile of $(e(u))_{u\geqslant 0}$ and $(\widetilde{e}(u))_{u\geqslant 0}$ via certain character sums over Fermat quotients, the authors of [30,33] determined the *linear complexity* (see below for the definition) of $(e(u))_{u\geqslant 0}$ and $(\widetilde{e}(u))_{u\geqslant 0}$ if 2 is a primitive element modulo p^2, and later the authors of [26,27,29] extended to a more general setting of $2^{p-1} \not\equiv 1 \pmod{p^2}$, the authors of [26,31] also determined the trace representations and the *k-error linear complexity* (see below for the definition) of $(e(u))_{u\geqslant 0}$ and $(\widetilde{e}(u))_{u\geqslant 0}$, respectively. The authors of [32] extended [27] further to determine the linear complexity of $(e(u))_{u\geqslant 0}$ when $r > 1$ under the assumption of $2^{p-1} \not\equiv 1 \pmod{p^2}$. We refer the reader to related references for details. All results indicate that such sequences have desirable cryptographic features.

Hence in this paper, we describe the Euler quotient $Q_r(u)$ as the p-adic decomposition

$$Q_r(u) = a_0(u) + a_1(u)p + \cdots + a_{r-1}(u)p^{r-1},\ u \geqslant 0,$$

where $0 \leqslant a_j(u) < p$ for $0 \leqslant j \leqslant r-1$, and consider the linear complexity of the level sequences $(a_j(u))_{u\geqslant 0}$ over $\mathbb{F}_p$ via introducing a new quotient, which coincides with the level sequences $(a_j(u))_{u\geqslant 0}$. Our second aim is to determine the k-error linear complexity for certain binary sequences defined by the level sequences $(a_j(u))_{u\geqslant 0}$ of the Euler quotient $Q_r(u)$.

We conclude this section by recalling the notions of the linear complexity and the k-error linear complexity. Let $\mathbb{F}$ be a field. For a T-periodic sequence $(s(u))_{u\geqslant 0}$ over $\mathbb{F}$, we recall that the *linear complexity* over $\mathbb{F}$, denoted by $\mathrm{LC}^{\mathbb{F}}((s(u))_{u\geqslant 0})$, is the least order L such that $(s(u))_{u\geqslant 0}$ satisfies

$$s(u+L) = c_{L-1}s(u+L-1) + \cdots + c_1 s(u+1) + c_0 s(u) \quad \text{for } u \geqslant 0,$$

where $c_0 \neq 0,\ c_1, \ldots, c_{L-1} \in \mathbb{F}$. Let

$$S(X) = s(0) + s(1)X + s(2)X^2 + \cdots + s(T-1)X^{T-1} \in \mathbb{F}[X],$$

which is called the *generating polynomial* of $(s(u))_{u\geqslant 0}$. Then the linear complexity over $\mathbb{F}$ of $(s(u))_{u\geqslant 0}$ is computed by

$$\mathrm{LC}^{\mathbb{F}}((s(u))_{u\geqslant 0}) = T - \deg\left(\gcd(X^T - 1,\ S(X))\right), \tag{6}$$

see, e.g. [35,36] for details. For integers $k \geqslant 0$, the *k-error linear complexity* over $\mathbb{F}$ of $(s(u))_{u\geqslant 0}$, denoted by $\mathrm{LC}_k^{\mathbb{F}}((s(u))_{u\geqslant 0})$, is the smallest linear complexity (over $\mathbb{F}$) that can be obtained by changing at most k terms of the sequence per period, see [37, 38], and see [39] for the related even earlier defined *sphere complexity*. Clearly $\mathrm{LC}_0^{\mathbb{F}}((s(u))_{u\geqslant 0}) = \mathrm{LC}^{\mathbb{F}}((s(u))_{u\geqslant 0})$ and

$$T \geqslant \mathrm{LC}_0^{\mathbb{F}}((s(u))_{u\geqslant 0}) \geqslant \mathrm{LC}_1^{\mathbb{F}}((s(u))_{u\geqslant 0}) \geqslant \cdots \geqslant \mathrm{LC}_l^{\mathbb{F}}((s(u))_{u\geqslant 0}) = 0,$$

where l equals the number of nonzero terms of $(s(u))_{u\geqslant 0}$ per period, i.e., the weight of $(s(u))_{u\geqslant 0}$.

The linear complexity and the k-error linear complexity are important cryptographic characteristics of sequences and provide information on the predictability and thus unsuitability for cryptography. For a sequence to be cryptographically strong, its linear complexity should be large, but not significantly reduced by changing a few terms. And according to the Berlekamp-Massey algorithm [40], the linear complexity should be large enough.

2 A new quotient

In this section, we introduce a new quotient to represent the level sequences of the Euler quotient $Q_r(u)$.

For integers $r > s > 0$, we can check

$$Q_r(u) \equiv Q_s(u) \pmod{p^s}, \quad u \geqslant 0. \tag{7}$$

In fact, for $p|u$ we have $Q_r(u) = Q_s(u) = 0$ by the assumption of (3). Now we suppose $\gcd(u, p) = 1$. Let

$$u^{\varphi(p^s)} = 1 + b_1 p^s + b_2 p^{2s} + \cdots \in \mathbb{Z}, \quad 0 \leqslant b_1, b_2, \ldots < p^s,$$

we see that $Q_s(u) = b_1$ by (2). On the other hand, we verify

$$u^{\varphi(p^r)} = (u^{\varphi(p^s)})^{p^{r-s}} = (1 + b_1 p^s + b_2 p^{2s} + \cdots)^{p^{r-s}} = 1 + b_1 p^r + (b_1^2 b_2 (p^{r-s} - 1)/2) p^{r+s} + \cdots \in \mathbb{Z},$$

from which we derive

$$\frac{u^{\varphi(p^r)} - 1}{p^r} = b_1 + (b_1^2 b_2 (p^{r-s} - 1)/2) p^s + \cdots.$$

We get $Q_r(u) \equiv b_1 \pmod{p^s}$. Hence we prove (7).

From (7), for integer $r \geqslant 2$ one can define a new quotient from $\mathbb{Z}_{p^{r+1}}$ (the additive group of numbers modulo p^{r+1}) to $\mathbb{Z}_p$ (the additive group of numbers modulo p) by

$$H_{r-1}(u) \equiv \frac{Q_r(u) - Q_{r-1}(u)}{p^{r-1}} \pmod{p}, \quad 0 \leqslant H_{r-1}(u) < p, \quad u \geqslant 0. \tag{8}$$

Indeed, we can write

$$Q_r(u) = Q_{r-1}(u) + H_{r-1}(u) p^{r-1},\ u \geqslant 0$$

and hence

$$Q_r(u) = H_0(u) + H_1(u) p + \cdots + H_{r-1}(u) p^{r-1},\ u \geqslant 0$$

by induction on $r-1$, where $H_0(u) = Q_1(u)$ by (7). Hence $(H_i(u))_{u\geqslant 0}$ is indeed the highest level sequence of $(Q_{i+1}(u))_{u\geqslant 0}$ for $i \geqslant 1$.

For example, if $r = 2$ and

$$u^{p-1} = 1 + c_1 p + c_2 p^2 + \cdots \in \mathbb{Z}, \quad 0 \leqslant c_1, c_2, \ldots < p,$$

we have $Q_1(u) = c_1$ and $Q_2(u) = c_1 + (\frac{p-1}{2} c_1^2 c_2)p \pmod{p^2}$, and hence

$$H_0(u) = c_1, \quad H_1(u) \equiv \frac{p-1}{2} c_1^2 c_2 \pmod{p}.$$

For $p|u$, we have $H_0(u) = H_1(u) = 0$.

Since the ith level sequence of $(Q_r(u))_{u \geqslant 0}$ is the highest level sequence of $(Q_{i+1}(u))_{u \geqslant 0}$ for $i \geqslant 0$, we only consider the highest level sequence of $(Q_r(u))_{u \geqslant 0}$ in the sequel, i.e., the quotient $H_{r-1}(u)$. Below we prove two simple properties for $H_{r-1}(u)$. We remark again that $H_0(u) = Q_1(u)$, which is the Fermat quotient.

Theorem 1. For any integers v, k and $r \geqslant 1$, we have

$$H_{r-1}(v + kp^r) \equiv H_{r-1}(v) - kv^{p-2} \pmod{p}.$$

Proof. For $r = 1$, $H_0(u)$ is the Fermat quotient $Q_1(u)$ and the result follows, see [11]. For $r > 1$, since the least period of $(Q_{r-1}(u))_{u \geqslant 0}$ is p^r, together with $v^p \equiv v \pmod{p}$ we get

$$\begin{aligned} H_{r-1}(v + kp^r) &\equiv \frac{Q_r(v + kp^r) - Q_{r-1}(v)}{p^{r-1}} \equiv \frac{Q_r(v) - Q_{r-1}(v)}{p^{r-1}} + k(p-1)v^{\varphi(p^r)-1} \\ &\equiv H_{r-1}(v) + k(p-1)v^{p-2} \pmod{p}. \end{aligned}$$

We complete the proof.

The least period of $(H_{r-1}(u))_{u \geqslant 0}$ follows from Theorem 1 directly.

Theorem 2. For integer $r \geqslant 1$, the least period of $(H_{r-1}(u))_{u \geqslant 0}$ is p^{r+1}.

We remark that Leeb [41] extended the Fermat quotients to introduce the notion of *Fermat quotients of order* $i \geqslant 1$ by defining

$$F^{(1)}(u) = Q_1(u)$$

and for $i > 1$

$$F^{(i)}(u) \equiv \frac{u^{p-1} - 1 - F^{(1)}(u)p - F^{(2)}(u)p^2 - \cdots - F^{(i-1)}(u)p^{i-1}}{p^i} \pmod{p}, \tag{9}$$

with $0 \leqslant F^{(i)}(u) < p$ for all integers u with $\gcd(u, p) = 1$ and $F^{(i)}(u) = 0$ otherwise. Indeed,

$$F^{(i)}(u) = c_i, \quad i \geqslant 1$$

for $\gcd(u, p) = 1$, if

$$u^{p-1} = 1 + c_1 p + c_2 p^2 + \cdots \in \mathbb{Z}, \quad 0 \leqslant c_1, c_2, \ldots < p.$$

We find that $F^{(i)}(u)$ is different from $H_{r-1}(u)$ defined in (8). (Note that Leeb introduced this definition for more general settings.)

3 Linear complexity of level sequences

In this section, we determine the exact value of the linear complexity of the highest-level sequence $(H_{r-1}(u))_{u \geqslant 0}$ of the Euler quotient $Q_r(u)$.

Theorem 3. For integers $r \geqslant 1$, the linear complexity (over the finite field $\mathbb{F}_p$) of the highest-level sequence $(H_{r-1}(u))_{u \geqslant 0}$ of Euler quotients in (1) and (3) satisfies

$$\mathrm{LC}^{\mathbb{F}_p}((H_{r-1}(u))_{u \geqslant 0}) = p^r + p - 1.$$

Proof. From Theorem 2, the least period of $(H_{r-1}(u))_{u\geqslant 0}$ is p^{r+1}. So for all integers $u \equiv i_0+i_1p+\cdots+i_rp^r \pmod{p^{r+1}}$ with $0 \leqslant i_0, i_1, \ldots, i_r < p$, we see that $(H_{r-1}(u))_{u\geqslant 0}$ can be represented by

$$H_{r-1}(i_0 + i_1p + \cdots + i_rp^r + jp^{r+1}) = \rho(i_0, i_1, \ldots, i_r) \ \text{ for } \ j \geqslant 0,$$

where the polynomial $\rho(X_0, X_1, \ldots, X_r) \in \mathbb{F}_p[X_0, X_1, \ldots, X_r]/\langle X_0^p - X_0, X_1^p - X_1, \ldots, X_r^p - X_r\rangle$ is of the form

$$\begin{aligned}&\rho(X_0, X_1, \ldots, X_r)\\ &\quad= \sum_{c_0=0}^{p-1}\sum_{c_1=0}^{p-1}\cdots\sum_{c_{r-1}=0}^{p-1} H_{r-1}(c_0 + c_1p + \cdots + c_{r-1}p^{r-1})\prod_{l=0}^{r-1}\big(1-(X_l-c_l)^{p-1}\big) - X_rX_0^{p-2},\end{aligned}$$

since

$$\begin{aligned}&H_{r-1}(i_0 + i_1p + \cdots + i_rp^r + jp^{r+1})\\ &\equiv H_{r-1}(i_0 + i_1p + \cdots + i_{r-1}p^{r-1}) - i_r(i_0 + i_1p + \cdots + i_{r-1}p^{r-1})^{p-2}\\ &\equiv \sum_{c_0=0}^{p-1}\sum_{c_1=0}^{p-1}\cdots\sum_{c_{r-1}=0}^{p-1} H_{r-1}(c_0 + c_1p + \cdots + c_{r-1}p^{r-1})\prod_{l=0}^{r-1}\big(1-(i_l-c_l)^{p-1}\big) - i_ri_0^{p-2} \pmod p\end{aligned}$$

by Theorem 1.

Then the degree of $\rho(X_0, X_1, \ldots, X_r)$ is $\deg(\rho) = p^r + p - 2$, see [42] for the definition of the degree of multi-variable polynomials. Hence by [42, Theorem 8], we have $\mathrm{LC}^{\mathbb{F}_p}((H_{r-1}(u))_{u\geqslant 0}) = \deg(\rho) + 1 = p^r + p - 1$.

The case of $r = 1$ in Theorem 3 has been reported in [11].

4 Linear complexity and *k*-error linear complexity of binary sequences derived from level sequences

In this section, we use the highest-level sequence $(H_{r-1}(u))_{u\geqslant 0}$ of the Euler quotient $Q_r(u)$ to define some families of binary sequences and determine their linear complexity and k-error linear complexity. Suppose that 2 is a primitive root modulo p^2. Then it is clear that 2 is also a primitive root modulo p^n for every $n \geqslant 1$, see e.g. [43].

From Theorem 1, the quotient $H_{r-1}(-)$ induces a surjective map from $\mathbb{Z}_{p^{r+1}}^*$ (the group of invertible elements modulo p^{r+1}) to $\mathbb{Z}_p$. Let

$$D_l = \{u : 0 \leqslant u < p^{r+1},\ \gcd(u, p) = 1,\ H_{r-1}(u) = l\}$$

for $l = 0, 1, \ldots, p-1$. We define a p^{r+1}-periodic binary sequence $(f(u))_{u\geqslant 0}$ by

$$f(u) = \begin{cases} 1, & \text{if } u \bmod p^{r+1} \in \cup_{l\in\mathcal{I}} D_l,\\ 0, & \text{otherwise,}\end{cases} \qquad u \geqslant 0, \tag{10}$$

where $\mathcal{I}$ is a non-empty subset of $\{0, 1, \ldots, p-1\}$. In particular, if $\mathcal{I} = \{\frac{p+1}{2}, \frac{p+1}{2}+1, \ldots, p-1\}$, $(f(u))_{u\geqslant 0}$ is the binary threshold sequence defined in (4) when $r = 1$ and if $\mathcal{I}$ is the set of quadratic non-residues modulo p, $(f(u))_{u\geqslant 0}$ is the binary sequence defined in (5) when $r = 1$ and $m = 2$.

Before we present main results of the linear complexity and k-error linear complexity for $(f(u))_{u\geqslant 0}$, we prove some auxiliary statements. Define

$$D_l(X) = \sum_{u\in D_l} X^u \in \mathbb{F}_2[X]$$

for $0 \leqslant l < p$.

Lemma 1. For $r \geqslant 1$, $0 \leqslant l < p$ and $1 \leqslant j \leqslant r$, the map $u \mapsto u \bmod p^j$ from D_l to $\mathbb{Z}_{p^j}^*$ is surjective and each element in $\mathbb{Z}_{p^j}^*$ exactly has p^{r-j} many pre-images in D_l.

Proof. For each $1 \leqslant v < p^r$ with $\gcd(v,p)=1$, the numbers $v+mp^r$ belong to different D_l $(0 \leqslant l < p)$ when m runs through the set $\{0,1,\ldots,p-1\}$ by Theorem 1, hence each D_l is of the form

$$D_l = \{v + m_{lv}p^r : \ 1 \leqslant v < p^r, \ \gcd(v,p)=1, \ m_{lv} = v(H_{r-1}(v) - l) \pmod p\}.$$

We will find that

$$D_l \bmod p^r = \{u \bmod p^r : u \in D_l\} = \mathbb{Z}_{p^r}^*, \quad 0 \leqslant l < p,$$

further we have

$$D_l \bmod p^j = \mathbb{Z}_{p^r}^* \bmod p^j = \mathbb{Z}_{p^j}^*, \quad 0 \leqslant l < p,$$

for $1 \leqslant j \leqslant r-1$. So the map $u \mapsto u \bmod p^j$ from D_l to $\mathbb{Z}_{p^j}^*$ is surjective and the number of pre-images of each element in $\mathbb{Z}_{p^j}^*$ can be calculated easily.

From the proof of Lemma 1, each D_l has the cardinality $|D_l| = p^{r-1}(p-1)$. Here and hereafter, we use $|S|$ to denote the cardinality of a set S.

Lemma 2. Let $r \geqslant 2$ and $\theta \in \overline{\mathbb{F}}_2$ with $\theta^{p^r} = 1$ but $\theta^p \neq 1$. For $0 \leqslant l < p$, we have

$$D_l(\theta) = 0.$$

Proof. We have

$$\sum_{u=0}^{p^r-1} \theta^u = \frac{1-\theta^{p^r}}{1-\theta} = 0$$

and

$$\sum_{u=0}^{p^{r-1}-1} \theta^{pu} = \frac{1-\theta^{p^r}}{1-\theta^p} = 0.$$

Then by Lemma 1, we derive

$$D_l(\theta) = \sum_{u \in \mathbb{Z}_{p^r}^*} \theta^u = \sum_{u=0}^{p^r-1} \theta^u - \sum_{u=0}^{p^{r-1}-1} \theta^{pu} = 0.$$

We complete the proof.

Lemma 3. Let $r \geqslant 2$ and $\theta \in \overline{\mathbb{F}}_2$ with $\theta^p = 1$. For $0 \leqslant l < p$, we have

$$D_l(\theta) = \begin{cases} 0, & \text{if } \theta = 1, \\ 1, & \text{otherwise.} \end{cases}$$

Proof. For $\theta \neq 1$, using Lemma 1 with $j=1$ we have

$$D_l(\theta) = p^{r-1} \sum_{u=1}^{p-1} \theta^u = \sum_{u=0}^{p-1} \theta^u - \theta^0 = \frac{1-\theta^p}{1-\theta} + 1 = 1.$$

For $\theta = 1$, we have $D_l(1) = p^{r-1}(p-1) = 0$ since $|D_l| = p^{r-1}(p-1)$.

Lemma 4. Let $\theta \in \overline{\mathbb{F}}_2$ with $\theta^p = 1$ but $\theta \neq 1$ and $G(X) \in \mathbb{F}_2[X]$ with $1 \leqslant \deg(G(X)) < p$. If 2 is a primitive root modulo p, we have

$$G(\theta) = 1 \Longleftrightarrow G(X) = X + X^2 + \cdots + X^{p-1}.$$

Proof. Since 2 is a primitive root modulo p, we see that $1 + X + X^2 + \cdots + X^{p-1}$ is the minimal irreducible polynomial with the root θ. So if $G(\theta) = 1$, we derive

$$(1 + X + X^2 + \cdots + X^{p-1}) | (G(X) - 1).$$

With the restriction on $\deg(G(X))$, we get $G(X) = X + X^2 + \cdots + X^{p-1}$. The converse is true after simple calculations.

Now we present our main result, which is a generalization of [31, Theorem 1] for the case of $r = 1$. However, we need more knowledge for the proof. Here we only assume $r \geqslant 2$.

Theorem 4. Let $r \geqslant 2$ and $(f(u))_{u\geqslant 0}$ be the binary sequence of period p^{r+1} defined in (10) using the highest-level sequence of Euler quotients in (1) and (3) and a non-empty subset $\mathcal{I}$ of $\{0, 1, \ldots, p-1\}$ with $1 \leqslant |\mathcal{I}| \leqslant (p-1)/2$. If 2 is a primitive root modulo p^2, then the k-error linear complexity over $\mathbb{F}_2$ of $(f(u))_{u\geqslant 0}$ satisfies

$$\mathrm{LC}_k^{\mathbb{F}_2}((f(u))_{u\geqslant 0}) = \begin{cases} p^{r+1} - p^r + p - 1, & \text{if } 0 \leqslant k < p^{r-1}, \\ p^{r+1} - p^r + 1, & \text{if } p^{r-1} \leqslant k < p^{r-1}(p-1), \\ p^{r+1} - p^r, & \text{if } p^{r-1}(p-1) \leqslant k < p^{r-1}(p-1)|\mathcal{I}|,\ |\mathcal{I}| > 1, \\ 0, & \text{if } k \geqslant p^{r-1}(p-1)|\mathcal{I}|, \end{cases}$$

if $|\mathcal{I}|$ is odd, and otherwise

$$\mathrm{LC}_k^{\mathbb{F}_2}((f(u))_{u\geqslant 0}) = \begin{cases} p^{r+1} - p^r, & \text{if } 0 \leqslant k < p^{r-1}(p-1)|\mathcal{I}|, \\ 0, & \text{if } k \geqslant p^{r-1}(p-1)|\mathcal{I}|. \end{cases}$$

Proof. Let

$$F_k(X) = \sum_{l\in\mathcal{I}} D_l(X) + e(X) \in \mathbb{F}_2[X] \tag{11}$$

be the generating polynomial of the sequence obtained from $(f(u))_{u\geqslant 0}$ by changing exactly k terms of $(f(u))_{u\geqslant 0}$ per period, where $e(X)$ is the corresponding error polynomial with k terms. $F_0(X)$ is in fact the generating polynomial of $(f(u))_{u\geqslant 0}$. It is easy to see that if k is equal to or larger than the Hamming weight of $(f(u))_{u\geqslant 0}$, the error linear complexity will reduce to zero. So we always suppose that $k < p^{r-1}(p-1)|\mathcal{I}|$ due to $|D_l| = p^{r-1}(p-1)$, in this case $F_k(X)$ is non-zero. We will consider the common roots of $F_k(X)$ and $X^{p^{r+1}} - 1$, the number of the common roots will help us to derive the values of k-error linear complexity of $(f(u))_{u\geqslant 0}$ by (6).

We divide all roots of $X^{p^{r+1}} - 1$ into four groups

$$\mathcal{G}_1 = \{\theta \in \overline{\mathbb{F}}_2 :\ \theta^{p^{r+1}} = 1,\ \theta^{p^r} \neq 1\},\ \ \mathcal{G}_2 = \{\theta \in \overline{\mathbb{F}}_2 :\ \theta^{p^r} = 1,\ \theta^p \neq 1\},$$
$$\mathcal{G}_3 = \{\theta \in \overline{\mathbb{F}}_2 :\ \theta^p = 1, \theta \neq 1\},\ \ \mathcal{G}_4 = \{1\}.$$

It is easy to check that $|\mathcal{G}_1| = p^{r+1} - p^r$, $|\mathcal{G}_2| = p^r - p$ and $|\mathcal{G}_3| = p - 1$.

First, all $\theta \in \mathcal{G}_1$ are roots of $\Phi(X) = 1 + X^{p^r} + X^{2p^r} + \cdots + X^{(p-1)p^r}$, which is irreducible since 2 is a primitive root modulo p^2. If $F_k(\theta) = 0$ for some $\theta \in \mathcal{G}_1$, we have

$$\Phi(X)|F_k(X)$$

and write

$$F_k(X) = \Phi(X)\pi(X). \tag{12}$$

Since

$$\deg(F_k(X)) = \deg(\Phi(X)) + \deg(\pi(X)),$$

we restrict $\deg(\pi(X)) < p^r$ and write

$$\pi(X) = X^{v_0} + X^{v_1} + \cdots + X^{v_{t-1}} \text{ with } 0 \leqslant v_0 < v_1 < \ldots < v_{t-1} < p^r,$$

where $t \geqslant 1$ since $F_k(X)$ is a nonzero polynomial. Then the exponent of each monomial in $\Phi(X)\pi(X)$ forms the set

$$\{v_j + lp^r :\ 0 \leqslant j \leqslant t-1,\ 0 \leqslant l \leqslant p-1\},$$

which can be divided into two sets A and B with

$$A = \{v_j + lp^r :\ 0 \leqslant j \leqslant t-1,\ 0 \leqslant l \leqslant p-1, v_j \neq 0,\ H_{r-1}(v_j + lp^r) \in \mathcal{I}\},$$

$$B = \{v_j + lp^r : \ 0 \leqslant j \leqslant t-1, \ 0 \leqslant l \leqslant p-1\} \setminus A.$$

By Theorem 1, A contains $|A|$ many numbers with

$$|A| = \begin{cases} (t-1)|\mathcal{I}|, & \text{if } v_0 = 0, \\ t|\mathcal{I}|, & \text{otherwise,} \end{cases}$$

and B contains $tp - |A|$ many numbers.

Hence, from (11) and (12), we find that the set of the exponents of monomials in $e(X)$ is

$$(\cup_{l\in\mathcal{I}} D_l \setminus A) \cup B,$$

the cardinality of which is

$$p^{r-1}(p-1)|\mathcal{I}| - |A| + |B| = p^{r-1}(p-1)|\mathcal{I}| + tp - \begin{cases} 2(t-1)|\mathcal{I}|, & \text{if } v_0 = 0, \\ 2t|\mathcal{I}|, & \text{otherwise.} \end{cases}$$

Due to $|\mathcal{I}| \leqslant (p-1)/2$ and $tp - 2t|\mathcal{I}| > 0$ we have

$$p^{r-1}(p-1)|\mathcal{I}| - |A| + |B| > p^{r-1}(p-1)|\mathcal{I}| > k,$$

However, it is impossible that $e(X)$ has $p^{r-1}(p-1)|\mathcal{I}|$ many terms and k terms simultaneously, a contradiction. So $\Phi(X) \nmid F_k(X)$, i.e.,

$$F_k(\theta) \neq 0, \ \text{for } \theta \in \mathcal{G}_1. \tag{13}$$

Second, we consider the case $\theta \in \mathcal{G}_2$. By Lemma 2 we get

$$F_k(\theta) = \begin{cases} 0, & \text{if } k = 0, \\ e(\theta), & \text{otherwise,} \end{cases} \quad \text{for } \theta \in \mathcal{G}_2. \tag{14}$$

Finally, we consider the case $\theta \in \mathcal{G}_3 \cup \mathcal{G}_4$. By Lemma 3 we get

$$F_k(\theta) = \begin{cases} |\mathcal{I}|, & \text{if } k = 0, \\ e(\theta) + |\mathcal{I}|, & \text{otherwise,} \end{cases} \quad \text{for } \theta \in \mathcal{G}_3 \tag{15}$$

and

$$F_k(\theta) = \begin{cases} 0, & \text{if } k = 0, \\ e(\theta), & \text{otherwise,} \end{cases} \quad \text{for } \theta \in \mathcal{G}_4. \tag{16}$$

Now we draw the following conclusions.

(i) If $|\mathcal{I}|$ is even, we find that

$$\mathrm{LC}_0^{\mathbb{F}_2}((f(u))_{u\geqslant 0}) = \mathrm{LC}^{\mathbb{F}_2}((f(u))_{u\geqslant 0}) = (p-1)p^r$$

and for any $1 \leqslant k < p^{r-1}(p-1)|\mathcal{I}|$, the number of the common roots of $F_k(X)$ and $X^{p^{r+1}} - 1$ will not increase by (13)–(16). So we have

$$\mathrm{LC}_k^{\mathbb{F}_2}((f(u))_{u\geqslant 0}) = (p-1)p^r, \ \text{ for } k < p^{r-1}(p-1)|\mathcal{I}|.$$

(ii) If $|\mathcal{I}|$ is odd, we find that

$$\mathrm{LC}_0^{\mathbb{F}_2}((f(u))_{u\geqslant 0}) = \mathrm{LC}^{\mathbb{F}_2}((f(u))_{u\geqslant 0}) = (p-1)p^r + p - 1.$$

Since 2 is a primitive root modulo p^2, we see that

$$\theta, \ \theta^2, \ \theta^{2^2}, \ldots, \ \theta^{2^{p^{r-1}(p-1)}-1} \in \mathcal{G}_2$$

are different for any $\theta \in \mathcal{G}_2$. If $e(\theta) \neq 0$ for some $\theta \in \mathcal{G}_2$, we have $e(\theta^{2^i}) \neq 0$ for $0 \leqslant i < p^{r-1}(p-1)$. That is to say, if such case occurs, there will be at least $p^{r-1}(p-1)$ many $\theta \in \mathcal{G}_2$ such that $e(\theta) \neq 0$ and hence the number of the common roots of $F_k(X)$ and $X^{p^{r+1}} - 1$ will not increase compared to the case $k = 0$ by (14). So according to (14)–(16), we need to find the smallest $k > 0$ such that the error polynomial $e(X)$ (with k terms) satisfies

$$e(\theta) = \begin{cases} 0, & \text{if } \theta \in \mathcal{G}_2, \\ 1, & \text{if } \theta \in \mathcal{G}_3, \\ 1, & \text{if } \theta \in \mathcal{G}_4, \end{cases} \tag{17}$$

and

$$e(\theta) = \begin{cases} 0, & \text{if } \theta \in \mathcal{G}_2, \\ 1, & \text{if } \theta \in \mathcal{G}_3, \\ 0, & \text{if } \theta \in \mathcal{G}_4, \end{cases} \tag{18}$$

respectively.

We firstly search for $e(X)$ satisfying (17) and consider $e(X)$ modulo $(X^{p^r} - 1)$. We note that $e(X) \not\equiv 0 \pmod{X^{p^r} - 1}$ since $e(\theta) = 1$ for $\theta \in \mathcal{G}_3 \cup \mathcal{G}_4$. Let

$$\Lambda(X) := \frac{X^{p^r} - 1}{X^p - 1} = 1 + X^p + X^{2p} + \cdots + X^{(p^{r-1}-1)p} \in \mathbb{F}_2[X].$$

Clearly $\Lambda(\theta) = 0$ for all $\theta \in \mathcal{G}_2$ and $\Lambda(\theta) = 1$ for all $\theta \in \mathcal{G}_3 \cup \mathcal{G}_4$. The facts that

$$X^p \Lambda(X) \equiv \Lambda(X) \pmod{X^{p^r} - 1}$$

and

$$e(X) \equiv \tau(X)\Lambda(X) \pmod{X^{p^r} - 1}$$

for some non-zero polynomial $\tau(X)$ with degree $< p$ guarantee that the error polynomial $e(X)$ with the smallest $k > 0$ terms satisfying (17) should be of the form

$$e(X) \equiv \Lambda(X) \equiv 1 + X^p + X^{2p} + \cdots + X^{(p^{r-1}-1)p} \pmod{X^{p^r} - 1}$$

and hence $k = p^{r-1}$. That is, when $k = p^{r-1}$ one can choose a suitable $e(X)$ as above such that the number of the common roots of $F_k(X)$ and $X^{p^{r+1}} - 1$ is equal to $p^r - 1$, and for any $k < p^{r-1}$, any $e(X)$ with k terms will not satisfy (17), this implies that the number of the common roots of $F_k(X)$ and $X^{p^{r+1}} - 1$ will not increase (compared to the case $k = 0$). So we derive

$$\mathrm{LC}_k^{\mathbb{F}_2}((f(u))_{u \geqslant 0}) = (p-1)p^r + p - 1 \quad \text{for} \quad k < p^{r-1}$$

and

$$\mathrm{LC}_k^{\mathbb{F}_2}((f(u))_{u \geqslant 0}) = (p-1)p^r + 1 \quad \text{for} \quad k = p^{r-1}.$$

Now we consider $e(X)$ satisfying (18). Following a similar way above, we derive by Lemma 4 that the error polynomial $e(X)$ with the smallest $k > 0$ terms satisfying (18) should be of the form

$$\begin{aligned} e(X) &\equiv (X + X^2 + \cdots + X^{p-1})\Lambda(X) \\ &\equiv (X + X^2 + \cdots + X^{p-1})(1 + X^p + X^{2p} + \cdots + X^{(p^{r-1}-1)p}) \pmod{X^{p^r} - 1} \end{aligned}$$

and hence the smallest $k = p^{r-1}(p-1)$. That is, when $k = p^{r-1}(p-1)$ a suitable $e(X)$ as of the form above guarantees that the largest number of the common roots of $F_k(X)$ and $X^{p^{r+1}} - 1$ is equal to p^r. So we derive

$$\mathrm{LC}_k^{\mathbb{F}_2}((f(u))_{u \geqslant 0}) = (p-1)p^r + 1 \quad \text{for} \quad p^{r-1} \leqslant k < p^{r-1}(p-1),$$

and

$$\mathrm{LC}_k^{\mathbb{F}_2}((f(u))_{u \geqslant 0}) = (p-1)p^r \quad \text{for} \quad p^{r-1}(p-1) \leqslant k < p^{r-1}(p-1)|\mathcal{I}|, \quad |\mathcal{I}| > 1.$$

We complete the proof.

Theorem 4 indicates the binary sequences are cryptographically strong. By the way, we mention here the sequences $(F^{(i)}(u))_{u\geqslant 0}$ of Fermat quotients of order $i \geqslant 1$ (9) and a construction of binary sequences defined by $(F^{(i)}(u))_{u\geqslant 0}$. It is easy to check that

$$F^{(i)}(v+kp^i) \equiv F^{(i)}(v) - kv^{p-2} \pmod p.$$

Following a similar proof of Theorem 3, we obtain

$$\mathrm{LC}^{\mathbb{F}_p}((F^{(i)}(u))_{u\geqslant 0}) = p^i + p - 1$$

for $i \geqslant 1$, also see a proof in [41] for a more general case. Define

$$\widetilde{D}_l^{(i)} = \{u : 0 \leqslant u < p^{i+1},\ \gcd(u,p) = 1,\ F^{(i)}(u) = l\}$$

for $l = 0, 1, \ldots, p-1$ and the p^{i+1}-periodic binary sequence $(f^{(i)}(u))_{u\geqslant 0}$ by

$$f^{(i)}(u) = \begin{cases} 1, & \text{if } u \pmod{p^{i+1}} \in \cup_{l\in\mathcal{I}} \widetilde{D}_l^{(i)}, \\ 0, & \text{otherwise,} \end{cases} \qquad u \geqslant 0,$$

where $\mathcal{I}$ is a non-empty subset of $\{0, 1, \ldots, p-1\}$ with $1 \leqslant |\mathcal{I}| \leqslant (p-1)/2$. If 2 is a primitive root modulo p^2, using a similar proof of Theorem 4 we have for $i \geqslant 2$

$$\mathrm{LC}_k^{\mathbb{F}_2}((f^{(i)}(u))_{u\geqslant 0}) = \begin{cases} p^{i+1} - p^i + p - 1, & \text{if } 0 \leqslant k < p^{i-1}, \\ p^{i+1} - p^i + 1, & \text{if } p^{i-1} \leqslant k < p^{i-1}(p-1), \\ p^{i+1} - p^i, & \text{if } p^{i-1}(p-1) \leqslant k < p^{i-1}(p-1)|\mathcal{I}|,\ |\mathcal{I}| > 1, \\ 0, & \text{if } k \geqslant p^{i-1}(p-1)|\mathcal{I}|, \end{cases}$$

if $|\mathcal{I}|$ is odd, and otherwise

$$\mathrm{LC}_k^{\mathbb{F}_2}((f^{(i)}(u))_{u\geqslant 0}) = \begin{cases} p^{i+1} - p^i, & \text{if } 0 \leqslant k < p^{i-1}(p-1)|\mathcal{I}|, \\ 0, & \text{if } k \geqslant p^{i-1}(p-1)|\mathcal{I}|. \end{cases}$$

For $i = 1$ the result above also holds, see [31].

5 Concluding remarks

In this paper, we define a new quotient, which coincides with the highest-level sequence of Euler quotients decomposed as p-adic numbers. We use this quotient to determine the exact values of linear complexity of the highest-level sequence of Euler quotients and values of k-error linear complexity for binary sequences derived from the highest-level sequences.

We note that there are $p^{r-1}(p-1)|\mathcal{I}|$ many 1's in one period of the constructed binary sequences. such sequences are not balanced. It is more frequent to define binary balanced sequences for some special applications. Unfortunately, we cannot construct balanced sequences in the way described in this paper when $r > 1$. However, we can modify the definition to reduce the imbalance as much as possible by defining

$$\widetilde{f}(u) = \begin{cases} 1, & \text{if } u \pmod{p^{r+1}} \in \cup_{l\in\mathcal{I}} D_l \cup P, \\ 0, & \text{otherwise,} \end{cases} \qquad u \geqslant 0,$$

where $P = \{ip : 0 \leqslant i < p^r\}$ and a non-empty subset $\mathcal{I}$ of $\{0, 1, \ldots, p-1\}$ with $1 \leqslant |\mathcal{I}| \leqslant (p-1)/2$. Together with

$$\sum_{u=0}^{p^r-1} \theta^{up} = \begin{cases} 0, & \text{if } \theta^{p^{r+1}} = 1 \text{ but } \theta^p \neq 1, \\ 1, & \text{if } \theta^p = 1, \end{cases} \quad \text{for } \theta \in \overline{\mathbb{F}}_2,$$

we can get exact values of k-error linear complexity of $(\widetilde{f}(u))_{u\geqslant 0}$ if 2 is a primitive root modulo p^2 by following the same way of the proof of Theorem 4.

Acknowledgements Niu Z H was partially supported by National Natural Science Foundation of China (Grant Nos. 61272096, 61202367), Shanghai Municipal Natural Science Foundation (Grant Nos. 13ZR1416100, 12ZR1443700) and State Scholarship Fund of China Scholarship Council. Chen Z X was partially supported by National Natural Science Foundation of China (Grant Nos. 61170246, 61373140) and State Scholarship Fund of China Scholarship Council. Du X N was partially supported by National Natural Science Foundation of China (Grants Nos. 61202395, 61462077) and Program for New Century Excellent Talents in University (NCET-12-0620). The authors wish to thank Arne Winterhof for sending us his student's thesis, the original version of [41]. Parts of this work were written during the pleasant visits of the first two authors to University of Kentucky in Lexington, USA. They wish to thank for the hospitality.

Conflict of interest The authors declare that they have no conflict of interest.

References

1 Agoh T, Dilcher K, Skula L. Fermat quotients for composite moduli. J Number Theory, 1997, 66: 29–50
2 Sha M. The arithmetic of Carmichael quotients. Period Math Hung, 2015, doi: 10.1007/s10998-014-0079-3
3 Bourgain J, Ford K, Konyagin S, et al. On the divisibility of Fermat quotients. Michigan Math J, 2010, 59: 313–328
4 Chang M C. Short character sums with Fermat quotients. Acta Arith, 2012, 152: 23–38
5 Chen Z X, Ostafe A, Winterhof A. Structure of pseudorandom numbers derived from Fermat quotients. In: Proceedings of the 3rd International Conference on Arithmetic of Finite Fields. Berlin: Springer-Verlag, 2010. 73–85
6 Chen Z X, Winterhof A. On the distribution of pseudorandom numbers and vectors derived from Euler-Fermat quotients. Int J Number Theory, 2012, 8: 631–641
7 Chen Z X, Winterhof A. Additive character sums of polynomial quotients. Contemp Math, 2012, 579: 67–73
8 Chen Z X, Winterhof A. Interpolation of Fermat quotients. SIAM J Discr Math, 2014, 28: 1–7
9 Ernvall R, Metsänkylä T. On the p-divisibility of Fermat quotients. Math Comput, 1997, 66: 1353–1365
10 Gómez-Pérez D, Winterhof A. Multiplicative character sums of Fermat quotients and pseudorandom sequences. Period Math Hungar, 2012, 64: 161–168
11 Ostafe A, Shparlinski I E. Pseudorandomness and dynamics of Fermat quotients. SIAM J Discr Math, 2011, 25: 50–71
12 Shparlinski I E. Character sums with Fermat quotients. Quart J Math, 2011, 62: 1031–1043
13 Shparlinski I E. Bounds of multiplicative character sums with Fermat quotients of primes. Bull Aust Math Soc, 2011, 83: 456–462
14 Shparlinski I E. On the value set of Fermat quotients. Proc Amer Math Soc, 2012, 140: 1199–1206
15 Shparlinski I E. Fermat quotients: Exponential sums, value set and primitive roots. Bull Lond Math Soc, 2011, 43: 1228–1238
16 Shparlinski I E, Winterhof A. Distribution of values of polynomial Fermat quotients. Finite Fields Appl, 2013, 19: 93–104
17 Fan S Q, Han W B. 0, 1 distribution in the highest level sequences of primitive sequences over $\mathbb{Z}/(2^e)$. Sci China Ser A-Math, 2003, 46: 516–524
18 Fan S Q, Han W B. Random properties of the highest level sequences of primitive sequences over $\mathbb{Z}/(2^e)$. IEEE Trans Inf Theory, 2003, 49: 1553–1557
19 Zheng Q X, Qi W F. Distribution properties of compressing sequences derived from primitive sequences over $\mathbb{Z}/(p^e)$. IEEE Trans Inf Theory, 2010, 56: 555–563
20 Zheng Q X, Qi W F, Tian T. On the distinctness of binary sequences derived from primitive sequences modulo square-free odd integers. IEEE Trans Inf Theory, 2013, 59: 680–690
21 Zhu X Y, Qi W F. Uniqueness of the distribution of zeroes of primitive level sequences over $\mathbb{Z}/(p^e)$. Finite Fields Appl, 2005, 11: 30–44
22 Zhu X Y, Qi W F. Uniqueness of the distribution of zeroes of primitive level sequences over $\mathbb{Z}/(p^e)$. II. Finite Fields Appl, 2007, 13: 230–248
23 Qi W F, Zhou J J. Distribution of 0 and 1 in the highest level of primitive sequences over $\mathbb{Z}/(2^e)$. Sci China Ser A-Math, 1997, 40: 606–611
24 Tian T, Qi W F. Periods of termwise exclusive ors of maximal length FCSR sequences. Finite Fields Appl, 2009, 15: 214–235
25 Aly H, Winterhof A. Boolean functions derived from Fermat quotients. Cryptogr Commun, 2011, 3: 165–174
26 Chen Z X. Trace representation and linear complexity of binary sequences derived from Fermat quotients. Sci China Inf Sci, 2014, 57: 112109
27 Chen Z X, Du X N. On the linear complexity of binary threshold sequences derived from Fermat quotients. Des Codes Cryptogr, 2013, 67: 317–323
28 Chen Z X, Du X N, Marzouk R. Trace representation of pseudorandom binary sequences derived from Euler quotients.

Appl Algebra Eng Commun Comput, 2015, doi: 10.1007/s00200-015-0265-4
29 Chen Z X, Gómez-Pérez D. Linear complexity of binary sequences derived from polynomial quotients. In: Proceedings of the 7th International Conference on Sequences and Their Application. Berlin: Springer-Verlag, 2012. 181–189
30 Chen Z X, Hu L, Du X N. Linear complexity of some binary sequences derived from Fermat quotients. Chin Commun, 2012, 9: 105–108
31 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
32 Du X N, Chen Z X, Hu L. Linear complexity of binary sequences derived from Euler quotients with prime-power modulus. Inform Process Lett, 2012, 112: 604–609
33 Du X N, Klapper A, Chen Z X. Linear complexity of pseudorandom sequences generated by Fermat quotients and their generalizations. Inform Process Lett, 2012, 112: 233–237
34 Wu C H, Chen Z X, Du X N. Binary threshold sequences derived from Carmichael quotients with even numbers modulus. IEICE Trans Fund Electron Commun Comput Sci, 2012, E95-A: 1197–1199
35 Cusick T W, Ding C S, Renvall A. Stream Ciphers and Number Theory. Amsterdam: North-Holland Publishing Co., 1998
36 Lidl R, Niederreiter H. Finite Fields. 2nd ed. Cambridge: Cambridge University Press, 1997
37 Meid W. How many bits have to be changed to decrease the linear complexity? Des Codes Cryptogr, 2004, 33: 109–122
38 Stamp M, Martin C F. An algorithm for the k-error linear complexity of binary sequences with period 2^n. IEEE Trans Inf Theory, 1993, 39: 1398–1401
39 Ding C S, Xiao G Z, Shan W J. The Stability Theory of Stream Ciphers. Berlin: Springer-Verlag, 1991
40 Massey J L. Shift register synthesis and BCH decoding. IEEE Trans Inf Theory, 1969, 15: 122–127
41 Leeb W. Linear complexity of extensions of Fermat quotients. In: Proceedings of the 83rd Workshop on General Algebra and the 27th Conference of Young Algebraists, Novi Sad, 2012
42 Blackburn S R, Etzion T, Paterson K G. Permutation polynomials, de Bruijn sequences, and linear complexity. J Comb Theory Ser A, 1996, 76: 55–82
43 Nathanson M B. Elementary Methods in Number Theory. New York: Springer-Verlag, 2000