Linear Complexity of r-ary Sequences Derived from Euler Quotients Modulo $2p$

Rayan Mohammed, Xiaoni Du$^{(\boxtimes)}$, and Li Li

College of Mathematics and Statistics, Northwest Normal University,
Lanzhou 730070, Gansu, People's Republic of China
ymLdxn@126.com

Abstract. Based on the Euler quotient modulo $2p$ (p is an odd prime), we extend the binary sequence with period $2p^2$ to r-ary sequence where r is an odd prime divisor of $(p-1)$. We determine exact values of the linear complexity of the new sequences under the assumption $r^{p-1} \not\equiv 1 \pmod{p^2}$, which are larger than half of the period. For cryptographic purpose, the linear complexities of the sequences in this paper are of desired values.

Keywords: r-ary sequences · Euler quotients · Linear complexity · Finite fields

1 Introduction

With the explosion of multimedia data, more and more data owners would outsource their personal multimedia data on the cloud [17,18]. Secure message transmission plays an main role in the information-based society. Pseudo-random sequences used for stream ciphers are required to have the properties of unpredictability. Linear complexity is one of the main components that indicates this feature. The linear complexity of a sequence is defined as the length of the shortest linear feedback shift register that can generate the sequence [14]. Due to the Berlekamp-Massey algorithm, it is reasonable to suggest that the linear complexity of a good sequence should be at least a half of the period. In the recent years, the sequence derived from the Euler quotients modulo an odd prime power, which is an extension of the Fermat quotients, are a hot spot and much of the sequences possess sound linear complexity, see [1–9,11,12,15,20] and the references therein. While for the study of the sequences derived from the Euler quotients modulo an even number are very rare. For the binary threshold sequence, the linear complexity is derived from Carmichael quotients with even numbers modulus in [16]. In [19], Zhang et al. promoted a class of binary sequences derived from Euler quotients with period $2p^2$ and p is an odd prime and determined the linear complexity and trace function representation of the sequences.

Supported by National Natural Science Foundation of China (61763044).

X. Sun et al. (Eds.): ICAIS 2019, LNCS 11634, pp. 104–112, 2019.
https://doi.org/10.1007/978-3-030-24271-8_10

For an odd prime p and integer $u \geq 0$ with $\gcd(u, 2p) = 1$, the Euler quotient $q_{2p}(u)$ modulo $2p$ can be defined as unique integer with

$$q_{2p}(u) \equiv \frac{u^{p-1} - 1}{2p} \pmod{2p}, \quad 0 \leq q_{2p}(u) \leq 2p - 1,$$

and $q_{2p}(u) = 0$ for $u \in R = \mathbb{Z}_{2p^2} \setminus \mathbb{Z}^*_{2p^2}$, where $\mathbb{Z}_{2p^2}$ denote by the ring of the all the integers modulo $2p^2$ and $\mathbb{Z}^*_{2p^2}$ of the multiplicative group of all the unit in $\mathbb{Z}_{2p^2}$ respectively.

The binary threshold sequence (e_u) defined in [19] as

$$e_u = \begin{cases} 0, & \text{if} \quad 0 \leq \frac{q_{2p}(u)}{2p} < \frac{1}{2}, \\ 1, & \text{if} \quad \frac{1}{2} \leq \frac{q_{2p}(u)}{2p} < 1, \end{cases} \qquad u \geq 0. \tag{1}$$

Motivated by the previous work in [15,19], we extend the binary threshold sequence to r-ary sequence as the following

$$f_u = \begin{cases} 0, & \text{if} \quad 0 \leq \frac{q_{2p}(u)}{2} \leq s, \\ 1, & \text{if} \quad s+1 \leq \frac{q_{2p}(u)}{2} \leq 2s, \\ \vdots & \vdots \\ r-1, & \text{if} \quad (r-1)s+1 \leq \frac{q_{2p}(u)}{2} \leq p-1, \end{cases} \tag{2}$$

where r is a prime, $r|(p-1)$ and $s = (p-1)/r$. In fact, if $r = 2$, then (f_u) is the binary threshold sequence defined in (1). We note that (f_u) is $2p^2$-periodical since $q_{2p}(u)$ is a $2p^2$-periodic sequence modulo $2p$ by the fact

$$q_{2p}(u + 2kp) \equiv \ q_{2p}(u) + k(p-1)u^{-1} \pmod{2p}, \ \gcd(u, 2p) = 1.$$

The linear complexity is considered as a primary quality measure for periodic sequences and play an important role in applications of sequences in cryptography. The main aims of this article is to determine the linear complexity of (f_u). We recall that the linear complexity $L((s_u))$ of a T-periodic sequence (s_u) with terms in finite field $\mathbb{F}_q$ with q elements is the least order of L of a linear recurrence relation over $\mathbb{F}_q$

$$s_{u+L} + c_{L-1}s_{u+L-1} + \cdots + c_1 s_{u+1} + c_0 s_u = 0 \quad \text{for } u \geq 0$$

which is satisfied by (s_u) and where $c_0 \neq 0, c_1, \ldots, c_{L-1} \in \mathbb{F}_q$. The polynomial

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

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

$$S(x) = s_0 + s_1 x + s_2 x^2 + \cdots + s_{T-1}x^{T-1} \in \mathbb{F}_q[x].$$

It is easy to show that

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

hence

$$L((s_u)) = T - \deg(\gcd(x^T - 1, S(x))), \tag{3}$$

which is the degree of minimal polynomial, see [13] for more details.

2 Preliminary

The main aims of this article are to determine the linear complexity of (f_u) under the assumption $r^{p-1} \not\equiv 1 \pmod{p^2}$. To achieve our goals we need to describe (f_u) in an equivalent way. For any subset $D \subset \mathbb{Z}_N$, define $aD = \{a \cdot b \pmod{N} : b \in N\}$ for any integer a.

If $\gcd(u, 2p) = 1$, it is easy to verify that

$$q_{2p}(uv) \equiv q_{2p}(u) + q_{2p}(v) \pmod{2p},\ \gcd(uv, 2p) = 1. \tag{4}$$

By [19], note that $q_{2p}(u)$ is always even since it can be rewritten as

$$q_{2p}(u) \equiv \frac{(u^{\frac{p-1}{2}} - 1)(u^{\frac{p-1}{2}} + 1)}{2p} \pmod{2p},$$

and two numbers $u^{\frac{p-1}{2}} \pm 1$ are even. Thus we define

$$D_l = \{u : q_{2p}(u) = 2l \pmod{2p} \text{ for } u \in \mathbb{Z}_{2p^2}^*\}$$

for $l = 0, 1, \ldots, p-1$. We always assume that g be a fixed primitive root modulo $2p^2$ such that $q_{2p}(g) = 2$, we declare such g exists. Otherwise, if $q_{2p}(g) = 2a \neq 2$. It is easy to prove that $\gcd(a, p) = 1$. By (4) we get $q_{2p}(g^{a^{-1}}) = 2$, where a^{-1} is the inverse of a modulo p. Furtherly, we have

$$q_{2p}(g^{a^{-1}+kp}) \equiv 2 \pmod{2p}$$

for all $0 \leq k < p-1$, then we have

$$D_0 = \{g^{kp} \pmod{2p^2} : 0 \leq k \leq p-2\}$$

is a subgroup of the multiplicative group $\mathbb{Z}_{2p^2}^*$ and for all $0 \leq l \leq p-1$, there exists $0 \leq l_0 \leq p-1$, such that

$$D_l = g^{l_0} D_0 = \{g^{l_0} \cdot a \pmod{2p} \ : \ a \in D_0\}$$

and each D_l has the cardinality $\#D_l = p-1$ and $\mathbb{Z}_{2p^2}^* = \bigcup_{l=0}^{p-1} D_l$.

Now the sequence (f_u) can be written equivalently as

$$f_u = \begin{cases} 0, & \text{if} \quad u \in D_0 \cup D_1 \cup \cdots \cup D_s \cup R, \\ 1, & \text{if} \quad u \in D_{s+1} \cup D_{s+2} \cup \cdots \cup D_{2s}, \\ \vdots & \vdots \\ r-1, & \text{if} \quad u \in D_{(r-1)s+1} \cup D_{(r-1)s+2} \cup \cdots \cup D_{p-1}. \end{cases} \tag{5}$$

Below, we are devoted to determining the linear complexity of the sequences. The rest of paper is organized as follows. In Sect. 3, we present some Auxiliary lemmas. In Sect. 4, We prove the main results of the paper and give some examples. Finally we conclude the paper.

3 Auxiliary Lemmas

Let $\mathbb{F}_r = \{0, 1, \ldots, r-1\}$ be the finite field of order r and $\overline{\mathbb{F}}_r$ be the algebraic closure of $\mathbb{F}_r$. Below we always let $\beta \in \overline{\mathbb{F}}_r$ be a primitive $2p^2$-th root of unity and the subscripts of D are calculated modulo p.

The following two lemmas are given in [19].

Lemma 1. *For any $0 \le l < p$, if $a \pmod{2p^2} \in D_{l'}$, for some $0 \le l' < p$ we have*

$$D_l \pmod{p} = \{1, 2, \ldots, p-1\} \text{ and } aD_l = D_{l+l'},$$

where $D_l \pmod{p} = \{a \pmod{p} : a \in D_l\}$

Lemma 2. *Let n be a positive integer. Then*

$$\{u \pmod{p^n} : u \in \mathbb{Z}_{2p^n}^*\} = \mathbb{Z}_{p^n}^*.$$

From now we define

$$D_l(x) = \sum_{u \in D_l} x^u \in \mathbb{F}_r[x], \text{ for } 0 \le l \le p-1.$$

From the definition of (f_u) we obtain that the generating polynomial of (f_u) is

$$E(x) = \sum_{u=0}^{2p^2-1} f_u x^u = \sum_{j=1}^{r-1} j \sum_{i=js+1}^{(j+1)s} D_i(x) \in \mathbb{F}_r[x].$$

Lemma 3. *Let $\beta \in \overline{\mathbb{F}}_r$ be a primitive $2p^2$-th root of unity. Then we have*

(1) $D_l(\beta^v) = D_{l+l'}(\beta)$,
(2) $D_l(\beta^u) = D_l(\beta^v)$ and $E(\beta^u) = E(\beta^v)$,

where $u, v \in D_l$ for some $0 \le l \le p-1$.

Proof. From Lemma 1 and the definitions of $D_l(x)$ and $E(x)$, we can obtain the results.

Lemma 4. *Let $\beta \in \overline{\mathbb{F}}_r$ be a primitive $2p^2$-th root of unity.*

(1) For all $v \in \mathbb{Z}_{2p^2}^* \cup 2\mathbb{Z}_{p^2}^*$, we have

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

(2) For $0 \le l < p$, we have

$$D_l(\beta^{kp}) = \begin{cases} 0, & \text{if } \; k \equiv 0 \pmod{p}, \\ -1, & \text{if } \; k \equiv 0 \pmod{2}, (k, p) = 1. \end{cases}$$

Proof. (1) From the definition of β, we have

$$\begin{aligned}0 = \beta^{2p^2} - 1 &= (\beta - 1) \sum_{j\in\mathbb{Z}_{2p^2}} \beta^j = (\beta^2 - 1) \sum_{j\in 2\mathbb{Z}_{p^2}} \beta^j \\ &= (\beta^p - 1) \sum_{j\in p\mathbb{Z}_{2p}} \beta^j = (\beta^{2p} - 1) \sum_{j\in 2p\mathbb{Z}_p} \beta^j \\ &= (\beta^{p^2} - 1)(\beta^{p^2} + 1)\end{aligned}$$

(1) of the Lemma is proved by the fact that

$$\begin{aligned}\mathbb{Z}_{2p^2} &= \mathbb{Z}^*_{2p^2} \cup 2\mathbb{Z}^*_{p^2} \cup p\mathbb{Z}_{2p} \\ &= \mathbb{Z}^*_{2p^2} \cup 2\mathbb{Z}^*_{p^2} \cup 2p\mathbb{Z}_p \cup p\mathbb{Z}^*_{2p} \cup \{p^2\}.\end{aligned}$$

(2) If $k \equiv 0 \pmod p$, then $k = 0$ or p. It can be easy to see that

$$D_l(\beta^{kp}) = D_l(\beta^{0p}) = D_l(1) = \sum_{u\in D_l} 1^u = p - 1 \equiv 0 \pmod r$$

if $k = 0$, and

$$D_l(\beta^{kp}) = D_l(\beta^{p^2}) = D_l(-1) = \sum_{u\in D_l} (-1)^u = 0$$

if $k = p$ from the proof of (1).

If $k \equiv 0 \pmod 2$ with $(k, p) = 1$, we have β^2 is a primitive p^2-th root of unity, so

$$\{k : \ k \text{ is an even, with } (\mathrm{k}, \mathrm{p}) = 1\},$$

then by Lemma 1 and (1) of this lemma, we have

$$\begin{aligned}D_l(\beta^{kp}) &= \beta^{2p} + \beta^{4p} + \ldots + \beta^{2(p-1)} \\ &= \frac{\beta^{2p} - \beta^{2p^2}}{1 - \beta^{2p}} \\ &= \frac{\beta^{2p} - 1}{1 - \beta^{2p}} \\ &= -1 \pmod r.\end{aligned}$$

□

Lemma 5. *If* $r^{p-1} \not\equiv 1 \pmod{p^2}$, *then*

$$D_l(\beta^u) \neq 0$$

for all $0 \leq l \leq p - 1$ *and all* $u \in \mathbb{Z}^*_{2p^2} \cup 2\mathbb{Z}^*_{p^2}$.

Proof. Denote by $d := ord_{2p^2}(r)$ the multiplicative order of r modulo $2p^2$. Thus, $d \mid p(p-1)$ and $d \geq p$ and $r^i \not\equiv r^j \pmod{2p^2}$ for $0 \leq i < j \leq p-1$. Suppose that $r \in D_{l_0 \pmod p}$, using Lemma 1 we have $r^i \pmod{2p^2} \in D_{l_0}$ for all $0 \leq i \leq p-1$ and

$$D_0 \cup rD_0 (= D_{l_0}) \cup \cdots \cup r^{p-1} D_0 = D_0 \cup D_1 \cup \cdots \cup D_{p-1} = \mathbb{Z}_{2p^2}^*.$$

Meanwhile the minimal polynomial of β^a over $\mathbb{F}_r$ is given by

$$M(x) = \prod_{k=0}^{d-1} (x - \beta^{ar^k}).$$

Consequently, if there are some $0 \leq l' \leq p-1$ and some $a \in D_k$ such that $D_{l'}(\beta^a) = 0$, then $D_{l'}(\beta^{ar^t}) = 0$ for $0 \leq t \leq d-1$.

Note that

$$D_k \cup rD_k \cup \cdots \cup r^{p-1} D_k = \mathbb{Z}_{2p^2}^*$$

then by Lemma 3(2) we have

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

Furthermore, Lemma 3(1) leads to that $D_{l'}(\beta^a) = D_{l'+1}(\beta^{a'})$ for some $a' \in D_{k-1}$, we also have $D_{l'+1}(\beta^u) = 0$ for all $u \in \mathbb{Z}_{2p^2}^*$. Seeking this process continually, we will get that

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

By Lemma 2 and notice the fact that $\beta^{p^2} = -1$, we have that for any $l = 0, 1, \ldots, p-1$, the polynomial $D_l(x) \pmod{x^{p^2}+1}$ 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 $D_l(x) \pmod{x^{p^2}+1}$ 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 $\deg(D_{l'}(x) \pmod{x^{p^2}+1}) < p^2 - p$. 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 $u \in \mathbb{Z}_{2p^2}^*$, we always have $D_l(\beta^u) \neq 0$.

For the case of $u \in 2\mathbb{Z}_{p^2}$, by Lemmas 1 and 2, with the fact that $d = ord_{p^2}(r)$ and $(\beta^2)^{p^2} = 1$, following the above approach, we can get desired result. Thus we have finish the proof of the lemma. □

4 Linear Complexity

In this section, we determine the linear complexity of r-ary sequence (f_u) defined in (2) under the assumption $r^{p-1} \not\equiv 1 \pmod{p^2}$.

Theorem 1. *Let (f_u) be the $2p^2$-periodic r-ary sequence defined as in (2). If $r^{p-1} \not\equiv 1 \pmod{p^2}$, then the linear complexity $L((f_u))$ and the minimal polynomial $M(x)$ of (f_u) are given by*

$$L((f_u)) = 2p^2 - 2p$$

and

$$M(x) = (x^{2p^2} - 1)/(x^{2p} - 1)$$

respectively.

Proof. We prove this theorem by the following two facts.

(1) $E(\beta^u) \neq 0$ if $u \in \mathbb{Z}^*_{2p^2} \cup 2\mathbb{Z}^*_{p^2}$.
Suppose that there is some $a \in D_k$ for some $0 \leq k \leq p-1$ such that $E(\beta^a) = 0$, similar to the proof of Lemma 5, we have $E(\beta^u) = 0$ holds for all $u \in \mathbb{Z}^*_{2p^2}$. Then we get $E(\beta^{a'}) = E(\beta) = 0$ where $a' \in D_l$. It follows from Lemma 3 and after simple calculation that

$$E(\beta^{a'}) = \sum_{j=0}^{r-1}(j-1)\sum_{i=jl+1}^{(j+1)l} D_i(\beta) - D_0(\beta) + D_l(\beta).$$

Then by Lemma 4, we have

$$0 = -D_l(\beta) = E(\beta) - E(\beta^{a'}) = \sum_{j=0}^{p-1} D_j(\beta) - D_l(\beta).$$

This contradiction with Lemma 5. Then for all $u \in \mathbb{Z}^*_{2p^2}$, we always have $E(\beta^u) \neq 0$.
For all $u \in 2\mathbb{Z}^*_{p^2}$, the results follows directly from Lemma 3.4 in [10].

(2) $E(\beta^u) = 0$ if $u = kp, k \in \mathbb{Z}_{2p}$. Note that each D_l has $p-1$ many elements for $0 \leq l < p$ and $D_l \pmod{p} = \{1, 2, \ldots, p-1\}$. Then we have two cases. If $k = 0, p$, by Lemma 4 we have

$$E(\beta^{kp}) = E(\pm 1) = \sum_{j=1}^{r-1} j \sum_{i=jl+1}^{(j+1)l} D_i(\pm 1) \equiv 0,$$

and if $u = kp$ for $k \in \mathbb{Z}^*_{2p} \cup 2\mathbb{Z}^*_{p}$, we have

$$\begin{aligned}
E(\beta^u) &= \sum_{j=1}^{r-1} j \sum_{i=jl+1}^{(j+1)l} D_i(\beta^{kp}) \\
&= \sum_{j=1}^{r-1} j \sum_{i=jl+1}^{(j+1)l} (\beta^{pk} + \beta^{2pk} + \cdots + \beta^{(p-1)pk}) \\
&= (\beta^{pk} + \beta^{2pk} + \cdots + \beta^{(p-1)pk}) \sum_{j=1}^{r-1} j \sum_{i=jl+1}^{(j+1)l} 1
\end{aligned}$$

$$\begin{aligned} &= l(\beta^{pk} + \beta^{2pk} + \cdots + \beta^{(p-1)pk}) \sum_{j=1}^{r-1} j \\ &\equiv 0 \pmod{r}. \end{aligned}$$

Putting every thing together, we have $E(\beta^u) = 0$ if and only if $u \in \{kp : k \in \mathbb{Z}_{2p}\}$, that is, the number of common roots of $E(x)$ and $x^{2p^2} - 1$ is $2p$, so the linear complexity of (f_u) is $2p^2 - 2p$ by (3). Meanwhile, it is easy to see that the minimial polynomial $M(x)$ of (f_u) satisfies $M(x) = (x^{2p^2} - 1)/(x^{2p} - 1)$. □

Now we provide some examples of $2p^2$-periodic r-ary sequences (f_u) to show the applicability of Theorem 1:

p	r	$L((f_u))$	$L((f_u))$ satisfying
7	3	84	$2p^2 - 2p$
11	5	220	$2p^2 - 2p$
13	3	312	$2p^2 - 2p$
19	3	684	$2p^2 - 2p$
23	11	1012	$2p^2 - 2p$
29	7	1624	$2p^2 - 2p$
31	3 or 5	1860	$2p^2 - 2p$
43	3 or 7	3612	$2p^2 - 2p$

5 Conclusion

For cryptographic purpose, one should construct pseudorandom sequences with high linear complexity according to the Berlekamp-Massey algorithm [14], 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.

In this article, under the assumption $r^{p-1} \not\equiv 1 \pmod{p^2}$, we give the linear complexity of r-ary sequence derived from Euler quotients modulo $2p$ with p an odd prime. The results show that the linear complexity is equal to $2p^2 - 2p$, which is larger enough to resist the attack from the Berlekamp-Massey algorithm. For the case of $r^{p-1} \equiv 1 \pmod{p^2}$, we leave an open problem since such primes pair are rare.

References

1. Chen, Z.: Linear complexity of some binary sequences derived from Fermat quotients. China Commun. **9**(2), 105–110 (2012)
2. Chen, Z.: Trace representation and linear complexity of binary sequences derived from Fermat quotients. Sci. China Inf. Sci. **57**(11), 1–10 (2014)

3. Chen, Z., Du, X.: On the linear complexity of binary threshold sequences derived from Fermat quotients. Des. Codes Cryptogr. **67**(3), 317–323 (2013)
4. Chen, Z., Du, X., Marzouk, R.: Trace representation of pseudorandom binary sequences derived from Euler quotients. Appl. Algebr. Eng. Commun. Comput. **26**(6), 555–570 (2015)
5. Dai, Z., Gong, G., Song, H.: A trace representation of binary Jacobi sequences. Discrete Math. **309**(6), 1517–1527 (2009)
6. Dai, Z., Gong, G., Song, H., Ye, D.: Trace representation and linear complexity of binary e-th power residue sequences of period p. IEEE Trans. Inf. Theory **57**(3), 1530–1547 (2011)
7. Dai, Z., Gong, G., Song, H., Ye, D.: Trace representation and linear complexity of binary e-th residue sequences. In: International Workshop on Coding and Cryptography-WCC, pp. 121–133 (2003)
8. Du, X., Klapper, A., Chen, Z.: Linear complexity of pseudorandom sequences generated by Fermat quotients and their generalizations. Inf. Process. Lett. **112**, 233–237 (2012)
9. Du, X., Chen, Z., Hu, L.: Linear complexity of binary sequences derived from Euler quotients with prime-power modulus. Inf. Process. Lett. **112**(14–15), 604–609 (2012)
10. Du, X.: An extension of binary threshold sequences from Fermat quotients. Adv. Math. Commun. **10**(4), 745–754 (2016)
11. Golomb, S., Gong, G.: Signal Design for Good Correlation. Cambridge University Press, Cambridge (2015)
12. Jungnickel, D.: Finite Fields, Structure and Arithmetics. Biblographiches Institute, Mannheim (1993)
13. Lidl, R., Niederreiter, H.: Finite Fields. Cambridge University Press, Cambridge (1997)
14. Massey, J.L.: Shift register synthesis and BCH decoding. IEEE Trans. Inf. Theory **15**(1), 122–127 (1969)
15. Wu, C., Wei, W.: An extension of binary threshold sequences from Fermat quotients. Adv. Math. Commun. **10**(4), 743–752 (2016)
16. Wu, C., Chen, Z., Du, X.: Binary threshold sequences derived from Carmichael quotients with even numbers modulus. IEICE Trans. Fundam. Electron. Commun. Comput. Sci. **E95-A**(7), 1197–1199 (2012)
17. Xiong, L., Shi, Y.: On the privacy-preserving outsourcing scheme of reversible data hiding over encrypted image data in cloud computing. CMC: Comput. Mater. Contin. **55**(3), 523–539 (2018)
18. Xu, W., Xiang, S., Sachnev, V.: A cryptograph domain image retrieval method based on Paillier homomorphic block encryption. CMC: Comput. Mater. Contin. **055**(2), 285–295 (2018)
19. Zhang, J., Zhao, C.: Linear complexity and trace representation of sequences with period $2p^2$. In: IEEE International Symposium on Information Theory, pp. 2206–2210 (2018)
20. Zhao, L., Du, X., Wu, C.: Trace representation of the sequences derived from polynomial quotient. In: Sun, X., Pan, Z., Bertino, E. (eds.) ICCCS 2018. LNCS, vol. 11066, pp. 26–37. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-00015-8_3