Linear Complexity of A Family of Binary pq^2-periodic Sequences From Euler Quotients

Jingwei Zhang, Shuhong Gao and Chang-An Zhao*

Abstract

We first introduce a family of binary pq^2-periodic sequences based on the Euler quotients modulo pq, where p and q are two distinct odd primes and p divides $q-1$. The minimal polynomials and linear complexities are determined for the proposed sequences provided that $2^{q-1} \not\equiv 1 \mod q^2$. The results show that the proposed sequences have high linear complexities.

Index Terms

Cryptography, linear complexity, binary sequences, Euler quotients.

I. Introduction

We will begin by the following definition of the Euler quotient modulo a product of two distinct odd primes. Let p and q be two distinct odd primes. For a nonnegative integer t that is relatively prime to pq, the Euler quotient $\psi(t) \pmod{pq}$ is defined as a unique integer in $\mathbb{Z}_{pq}$ with

$$\psi(t) = \frac{t^{\varphi(pq)} - 1}{pq} \pmod{pq}, \quad (1)$$

where $\varphi(\cdot)$ is the well-known Euler-phi function. We also define $\psi(t) = 0$ if t and pq are not relatively prime.

J.W. Zhang is with School of Information Science, Guangdong University of Finance and Economics, Guangzhou, 510320, P.R. China (E-mail: jingweizhang@gdufe.edu.cn)

S. Gao is with School of Mathematical and Statistical Sciences, Clemson University, Clemson, S.C.,29634, U.S.A (E-mail: sgao@math.clemson.edu)

C.-A, Zhao is with School of Mathematics, Sun Yat-sen University, Guangzhou 510275, P.R.China and with Guangdong Key Laboratory of Information Security, Guangzhou 510006, P.R. China.. $*$ Corresponding author. (E-mail: zhaochan3@mail.sysu.edu.cn)

It can be seen easily that the Euler quotient has the following property:

$$\psi(t+kpq) \equiv \psi(t) + kt^{-1}(p-1)(q-1) \pmod{pq}. \tag{2}$$

where $t, k \in \mathbb{Z}$ and t is relatively prime to pq.

In 2010, Chen, Ostafe and Winterhof [11] introduced families of binary sequences using Fermat/Euler quotients. Since then several nice cryptographic properties of these sequences were proved in [3]–[8]. Based on the distribution and algebraic structure of the Fermat quotients, the linear complexity was determined for a binary threshold sequence defined from Fermat quotients [8]. Naturally, the definition of the Euler quotient can be generalized by the Euler's Theorem [1]. Chen and Winterhof extended the distribution of pseudorandom numbers and vectors derived from Fermat quotients to Euler quotients [6]. Moreover, linear complexities were calculated for binary sequences derived from Euler quotients with prime-power modulus. Trace representations and linear complexities were investigated for binary sequences derived from the Fermat quotient [3]. Subsequently, a trace representation was given for a family of binary sequences derived from Euler quotients modulo a fixed power of a prime [4]. Chen and Winterhof generalized the Fermat quotient to the polynomial quotient in [7]. Then the k-error linear complexity was determined for binary sequences derived from the polynomial quotient modulo a prime [5] or its power [22], respectively. In [23], a series of optimal families of perfect polyphase sequences were derived from the array structure of Fermat-quotient sequences. All of the above results show that pseudorandom sequences derived from Fermat quotients, Euler quotients or their variants can be regarded as an important class of sequences from a cryptographic point of view.

In this paper, we study binary sequences derived from the Euler quotient modulo pq. Using the same notation as above, a binary threshold sequence $\mathbf{s} = \{s_t | t \in \mathbb{Z}, t \geq 0\}$ from the Euler quotient modulo pq can be defined as

$$s_t = \begin{cases} 0, & \text{if} \quad 0 \leq \frac{\psi(t)}{pq} < \frac{1}{2}, \\ 1, & \text{if} \quad \frac{1}{2} \leq \frac{\psi(t)}{pq} < 1. \end{cases} \tag{3}$$

For our purpose, we introduce the concept of the linear complexity of binary sequences now. The linear complexity of an N-periodic sequence $\mathbf{a} = \{a_i | i \in \mathbb{Z}, i \geq 0\}$ over the binary field $\mathbb{F}_2$ is the smallest nonnegative integer L for which there exist elements $c_1, c_2, \cdots, c_L \in \mathbb{F}_2$ such that

$$a_i + c_1 \cdot a_{i-1} + \cdots + c_L \cdot a_{i-L} = 0, \ for\ all\ i \geq L.$$

Let $A(x) = \sum_{i=0}^{N-1} a_i x^i \in \mathbb{F}_2[x]$ be the generating polynomial of $\mathbf{a}$. By [12], the minimal polynomial of $\mathbf{a}$ is defined as

$$M_{\mathbf{a}}(x) = \frac{x^N - 1}{\gcd(x^N - 1, A(x))},$$

where $\gcd(\cdot, \cdot)$ denotes the greatest common divisor of two polynomials over $\mathbb{F}_2$ and the linear complexity of $\mathbf{a}$ is

$$\mathcal{L}(\mathbf{a}) = N - \deg(\gcd(x^N - 1, A(x))).$$

Note that the linear complexity is of fundamental importance as a complexity measure for binary sequences in sequences designs [12], [15], [16]. Besides the measure of the linear complexity for sequences, other measures are also required according to different specific requirements from applications, for example, low autocorrelation or cross-correlation [24], [25], good nonlinear properties [18], [26], [27], and k-error complexities [9], [10]. For a binary sequence to be cryptographically strong, the linear complexity of the sequence should be at least a half of the least period of the sequence in order to resist the attack of Berlekamp-Massey algorithm [12], [20].

The main contribution of this paper is to determine the minimal polynomial and the linear complexity of the sequence defined in (3). We state our main result as follows.

Theorem 1: Let p and q be two distinct odd primes with p dividing $q-1$. Assume that $2^{q-1} \not\equiv 1 \pmod{q^2}$. Then the binary threshold sequence $\mathbf{s}$ defined in (3) has period at least pq^2. The minimal polynomial of $\mathbf{s}$ is

$$M_{\mathbf{s}}(x) = \begin{cases} \Phi_{pq^2}(x), & \text{if} \quad q \equiv 1 \pmod 4, \\ \Phi_{pq^2}(x)\Phi_{pq}(x), & \text{if} \quad q \equiv 3 \pmod 4, \end{cases}$$

where $\Phi_n(x)$ denotes the n-th cyclotomic polynomial for any positive integer n and the linear complexity of $\mathbf{s}$ is

$$\mathcal{L}(\mathbf{s}) = \begin{cases} (p-1)(q^2-q), & \text{if} \quad q \equiv 1 \pmod 4, \\ (p-1)(q^2-1), & \text{if} \quad q \equiv 3 \pmod 4. \end{cases}$$

To the best of our knowledge, this is the first time to introduce this kind of sequences on basis of the Euler quotient modulo a product of two distinct odd primes. Under the condition that p divides $q-1$, we will show that the binary sequence has period at least pq^2. Furthermore, minimal polynomials and linear complexities of this class of binary sequences are determined. It turns out that the proposed sequences have high linear complexities and may be useful in cryptography and digital communications.

By using the generalized cyclotomic techniques, one can also construct other binary sequences with period pq^2. We refer the reader to see [2], [13], [17] for more details. We emphasize that our results are new. In particular, we point out that our results are not one special case of Theorem 4.2 of [17] although both may give a sequence with period pq^2. In fact, this can be seen easily by comparing linear complexities of the two families of binary sequences.

In the rest of the paper, we give a proof of the above theorem in Section II, and conclude with a few remarks in Section III.

II. Proof of Main Results

In this section, we are devoting to the proof of the main results.

We first show that pq^2 is one of the periods of sequence s under the condition that p is a divisor of $q-1$. Setting $k=q$ in (2), we see that

$$\psi(t+pq^2)=\psi(t) \pmod{pq}$$

which implies $s_{t+pq^2}=s_t$ for all $t\geq 0$. Thus the sequence s is periodic with period pq^2. We will demonstrate that pq^2 is the least period of the sequence s in the following lemma.

Lemma 1: With the notation above, the sequence s has period at least pq^2.

Proof: We first prove that pq is not a period of the sequence s. By (2), we have

$$\psi(pq+1)\equiv\psi(1)+(p-1)(q-1)\equiv(p-1)(q-1) \pmod{pq}.$$

It follows from $2(p-1)(q-1)-pq=(p-2)(q-1)-p>0$ that the $(pq+1)$-th term of the sequence s is equal to 1, i.e., $s_{pq+1}=1$. Note that $s_1=0\neq 1=s_{pq+1}$ according to the definition of the sequence s. Hence pq is not a period of the sequence s.

Now we prove that q^2 is not a period of the sequence s. We can assume that q^2 is a period of the sequence s. Let $k=\lceil\frac{pq}{2(p+q-1)}\rceil$. It follows from (2) that $\psi(-1+kpq)=k(p+q-1) \pmod{pq}$ and thus $s_{-1+kpq}=1$. This means that the sequence s satisfies $s_{-1+kpq+q^2}=s_{-1+kpq}=1$. However, we have $s_{-1+kpq+q^2}=0$ according to the definition of the sequence s and $\gcd(kpq-1+q^2,pq)=\gcd(kpq+(q-1)(q+1),pq)=p$. It follows that $s_{kpq-1+q^2}\neq s_{kpq-1}$, a contradiction.

Hence the least period of the sequence s is pq^2, which completes the proof of the lemma. ■

For any integer $n \geq 2$, we denote by $\mathbb{Z}_n = \{0, 1, \cdots, n-1\}$ all representatives for the residue classes of integers modulo n and by $\mathbb{Z}_n^*$ all representatives that are relatively prime to n in $\mathbb{Z}_n$, respectively. Since the least period of s is pq^2, we restrict the action of ψ on $\mathbb{Z}_{pq^2}$ sometimes. With a slight abuse of notation, we shall still use the same symbol ψ to denote this restriction of the Euler quotient on $\mathbb{Z}_{pq^2}$.

Let $g \in \mathbb{Z}_{pq^2}^*$ be a fixed common primitive root of both p and q^2. The Chinese Reminder Theorem(CRT) [14] guarantees that there exists an element h of $\mathbb{Z}_{pq^2}^*$ such that

$$\begin{cases} h \equiv g \pmod{p}, \\ h \equiv 1 \pmod{q^2}. \end{cases}$$

Put $d = \gcd(p-1, q-1)$ and $e = \text{lcm}(p-1, q-1) = (p-1)(q-1)/d$ where lcm denotes least common multiple. Then the unit group $\mathbb{Z}_{pq^2}^*$ of the ring $\mathbb{Z}_{pq^2}$ [13] can be written as follows

$$Z_{pq^2}^* = \{g^i h^j : 0 \leq i < qe, 0 \leq j < d\}. \tag{4}$$

The following lemma shows that the map ψ is a group homomorphism when we restrict the action of the map ψ to the unit group $\mathbb{Z}_{pq^2}^*$.

Lemma 2: Let $\psi : t \to \psi(t)$ be the map from $\langle \mathbb{Z}_{pq^2}^*, \cdot \rangle$ to $\langle p\mathbb{Z}_{pq}, + \rangle$, where $p\mathbb{Z}_{pq} = \{lp \mid 0 \leq l \leq q-1\}$ contains exactly all of the residue classes which are divisible by p in the addition group $\mathbb{Z}_{pq}$. Then ψ is a surjective group homomorphism.

Let g and h be defined as above. Then the image and kernel of ψ is given as

$$\text{Img}(\psi) = p\mathbb{Z}_{pq}$$

and

$$\text{Ker}(\psi) = \langle g^q, h \rangle = \{g^{qi} h^j\} \mid 0 \leq i < e, 0 \leq j < d\},$$

respectively.

Proof: Note that $t^{p-1} \equiv 1 \pmod{p}$ for $t \in \mathbb{Z}_{pq^2}^*$. We can write $t^{p-1} = 1 + t'p$ for some integer t'. Substituting it into (1), we have

$$\psi(t) = \psi(t) = \frac{(1 + t'p)^{q-1} - 1}{pq} \equiv t'(q-1)q^{-1} \equiv 0 \pmod{p}$$

as p divides $q - 1$. This means that $\psi(t)$ is divisible by p and thus the map ψ is well defined.

For $u, v \in \mathbb{Z}_{pq^2}^*$ it follows from the Euler's Theorem that

$$\begin{aligned}\psi(uv) =& \frac{(uv)^{\varphi(pq)} - 1}{pq} \\ =& \frac{(uv)^{\varphi(pq)} - u^{\varphi(pq)} + u^{\varphi(pq)} - 1}{pq} \\ =& u^{\varphi(pq)}\psi(v) + \psi(u) \\ \equiv& \psi(u) + \psi(v) \pmod{pq}\end{aligned}$$

which yields the map ψ is a group homomorphism.

Now we show that the map ψ is surjective. There exists some integer t_1 such that $g^{q-1} = 1+t_1q$ with $t_1 \not\equiv 0 \pmod q$ since g is a primitive root in $\mathbb{Z}_{q^2}^*$. This implies that

$$\psi(g) = \frac{g^{\varphi(pq)} - 1}{pq} \equiv \frac{(1 + t_1 q)^{p-1} - 1}{pq} \equiv t_1(p-1)p^{-1} \not\equiv 0 \pmod q.$$

Note that $\psi(g) \equiv 0 \pmod p$. It follows from the CRT that there exists some positive integer a with $a \in \mathbb{Z}_q^*$ such that

$$\psi(g) \equiv pa \not\equiv 0 \pmod{pq}.$$

It follows that pa is one generator of the addition group $p\mathbb{Z}_{pq}$. Consequently, the map ψ is surjective and $\text{Img}(\psi) = p\mathbb{Z}_{pq}$.

It is known that both $\psi(g)$ and $\psi(h)$ are divisible by p. Also,

$$\psi(g^q) = q\psi(g) = 0 \pmod q.$$

On the basis of the CRT, we have $\psi(g^q) = 0 \pmod{pq}$. Hence $g^q \in \text{Ker}(\psi)$. Observe that $h \equiv 1 \pmod{q^2}$. We can write $h = 1 + q^2 h_1$. Hence

$$\psi(h) = \frac{h^{\varphi(pq)} - 1}{pq} \equiv p^{-1}\frac{(1 + q^2 h_1)^{\varphi(pq)} - 1}{q} \equiv 0 \pmod q.$$

Combining the above equation with $\psi(h) = 0 \pmod p$, we get $h \in \text{Ker}(\psi)$. Therefore, we have

$$\{(g^q)^i h^j \pmod{pq^2} \mid 0 \le i < e, 0 \le j < d\} = \langle g^q, h\rangle \subseteq \text{Ker}(\psi).$$

Now we need to show that the kernal $\text{Ker}(\psi)$ and the subgroup $\langle g^q, h\rangle$ have the same cardinality. By the Third Isomorphism Theorem [21], we have

$$\mathbb{Z}_{pq^2}^*/\langle g^q, h\rangle \simeq \big(\langle g, h\rangle/\langle h\rangle\big)/\big(\langle g^q, h\rangle/\langle h\rangle\big) \simeq \langle g\rangle/\langle g^q\rangle.$$

This yields that $g^0\langle g^q, h\rangle, g^1\langle g^q, h\rangle, \cdots, g^{q-1}\langle g^q, h\rangle$ are all cosets of the subgroup $\langle g^q, h\rangle$ of $\mathbb{Z}^*_{pq^2}$. It follows that $|\langle g^q, h\rangle| = (p-1)(q-1)$. On the other hand, according to the Fundamental Homomorphism Theorem [21], we see that

$$|\text{Ker}(\psi)| = |\frac{\mathbb{Z}^*_{pq^2}}{\text{Img}(\psi)}| = \frac{(p-1)(q-1)q}{q} = (p-1)(q-1)$$

and so $\langle g^q, h\rangle = \text{Ker}(\psi)$. This completes the whole proof of the lemma. ■

Note that Lemma 2 gives that $\psi(g) = pa \pmod{pq}$ with some $a \in \mathbb{Z}^*_q$. This means that $\psi(g) = pa \pmod{q}$ by the CRT. Let b be the inverse of a in $\mathbb{Z}^*_q$, i.e., $ab \equiv 1 \pmod{q}$. Define $\hat{g} = g^b$ in $\mathbb{Z}^*_{pq^2}$. Then

$$\psi(\hat{g}) = b \cdot \psi(g) \pmod{pq}$$

by the homomorphism property of the map ψ. It follows from $\psi(g) \equiv pa \pmod{q}$ that

$$\psi(\hat{g}) \equiv pab \equiv p \pmod{q}.$$

Combining the above equality with $\psi(\hat{g}) = 0 \pmod{p}$, we get $\psi(\hat{g}) = p \pmod{pq}$. The following lemma describes a partition of $\mathbb{Z}^*_{pq^2}$ which will give a new explanation of the definition of the sequence s.

Lemma 3: Let $\hat{g}$ be an element in $\mathbb{Z}^*_{pq^2}$ with $\psi(\hat{g}) = p \pmod{pq}$. Define

$$D_\ell = \{t : \psi(t) = \psi(t) = p\ell \pmod{pq}, t \in Z^*_{pq^2}\}$$

and

$$\hat{D}_\ell = \hat{g}^\ell D_0 = \{\hat{g}^\ell \cdot t \pmod{pq} : t \in D_0\}$$

for $\ell = 0, 1, \cdots, q-1$. Then $\mathbb{Z}^*_{pq^2} = \bigcup_{\ell=0}^{q-1} D_\ell$ and $D_\ell = \hat{D}_\ell$ for all $\ell \in \mathbb{Z}_q$.

Proof: We first prove that $\hat{D}_\ell = D_\ell$ for all $\ell \in \mathbb{Z}_q$. Note that Lemma 2 gives that $D_0 = \text{Ker}(\psi)$. It is easy to see that for $\hat{g}^\ell t_0 \in \hat{D}_\ell$ with $t_0 \in D_0 = \text{Ker}(\psi)$ we have

$$\psi(\hat{g}^\ell t_0) = l \cdot \psi(\hat{g}) + \psi(t_0) = \ell p \pmod{pq}.$$

This implies that $\hat{D}_\ell \subseteq D_\ell$. Conversely, for $t \in D_\ell$, we have

$$\psi(t) = pl = l\psi(\hat{g}) = \psi(\hat{g}^\ell) \pmod{pq}$$

and thus

$$\psi(\frac{t}{\hat{g}^\ell}) = 0 \pmod{pq}$$

by the homomorphism property of ψ. This means that

$$\frac{t}{\hat{g}^{\ell}} \in \text{Ker}(\psi) = D_0.$$

Therefore, there exists some element $t_0 \in D_0$ such that

$$\frac{t}{\hat{g}^{\ell}} \equiv t_0 \pmod{pq}.$$

Hence we have $t = \hat{g}^{\ell} \cdot t_0 \in \hat{g}^{\ell} D_0 = \hat{D}_{\ell}$ and so $D_{\ell} = \hat{D}_{\ell}$. This completes the whole proof of the lemma. ■

By the definition of D_ℓ and $\hat{D}_\ell$, Lemma 3 gives that $|D_\ell| = |\hat{D}_\ell| = (p-1)(q-1)$ for $\ell = 0, 1, \cdots, q-1$. Let $P = \{t : t \in Z_{pq^2}, \gcd(t, pq) \neq 1\}$. The sequence s can be rewritten as

$$s_t = \begin{cases} 0, & \text{if} \quad t \in D_0 \cdots \cup D_{(q-1)/2} \cup P, \\ 1, & \text{if} \quad t \in D_{(q+1)/2} \cup \cdots D_{q-1}. \end{cases}$$

The new explanation of the sequence s will be helpful to determine linear complexities. We will make extensive use of the following lemmas for completing the proof of Theorem 1.

Lemma 4: *For any* $0 \le i < q$, *if* $u \pmod{pq^2} \in D_j$ *for some* $0 \le j < q$, *we have*

$$uD_i = \{uv \pmod{pq^2} : v \in D_i\} = D_{i+j}.$$

where all the subscripts are certainly understood modulo q. *In particular,* $D_{ri} = \hat{g}^r D_i$ *for* $0 \le r \le q-1$.

Proof: If $u \in D_j$ and $v \in D_i$, then $u = \hat{g}^j u_0$ and $v = \hat{g}^i v_0$ with $u_0,\ v_0 \in D_0$. Hence $uv = \hat{g}^{i+j} u_0 v_0 \in \hat{g}^{i+j} D_0 = D_{i+j}$. This implies that $uD_i \subseteq D_{i+j}$. Conversely, it can be seen easily that $D_{i+j} \subseteq uD_i$. This finishes the proof of the lemma. ■

The study of the behavior of the coset D_ℓ under modulo various divisors of pq^2 leads to a number of useful lemmas.

Lemma 5: *For* $0 \le \ell < q$, *we have the following two multiset equalities*

$$\{u \pmod{p} : u \in D_\ell\} = (q-1) * \mathbb{Z}_p^*,$$

where $(q-1) * \mathbb{Z}_p^*$ *is the multiset in which each element of* $\mathbb{Z}_p^*$ *appears with multiplicity* $q-1$, *and*

$$\{u \pmod{q} : u \in D_\ell\} = (p-1) * \mathbb{Z}_q^*,$$

where $(p-1) * \mathbb{Z}_q^*$ *is the multiset in which each element of* $\mathbb{Z}_q^*$ *appears with multiplicity* $p-1$.

Proof: For $u \in D_\ell$ with some fixed $\ell \in \mathbb{Z}_q$ it can be written as $u = \hat{g}^\ell g^{qi} h^j$ for $0 \le i < e$ and $0 \le j < d$. Recall that $\hat{g} = g^b$ with some fixed $b \in \mathbb{Z}_q^*$ in Lemma 3. Then $u = g^{qi+b\ell} h^j$ in $\mathbb{Z}_{pq^2}$ and so

$$u = \hat{g}^\ell g^{qi} h^j \equiv g^{qi+b\ell+j} \equiv g^{b\ell+j} \cdot (g^q)^i \pmod{p}.$$

According to $\gcd(p-1, q) = 1$, we see that g^q is also a primitive root of $\mathbb{Z}_p^*$. If we fix some $j_0 \in \mathbb{Z}_d$, then $(u \equiv g^{qi+b\ell+j_0} \pmod{p})$ runs through $\mathbb{Z}_p^*$ when i run throughs $\mathbb{Z}_e$. Now we count the multiplicity of each element in $\mathbb{Z}_p^*$ when i and j run through $\mathbb{Z}_e$ and $\mathbb{Z}_d$ respectively. Assume that

$$u \equiv g^{qi+b\ell+j_0} \equiv g^{a_0} \pmod{p}$$

where $0 \le a_0 \le p-2$. This means that

$$qi = a_0 - j_0 - b\ell \pmod{p-1}$$

for $i \in \mathbb{Z}_e$. According to $\gcd(p-1, q) = 1$, it is equivalent to

$$i \equiv q^{-1}(a_0 - j_0 - b\ell) \pmod{p-1}.$$

There exists $\frac{q-1}{d}$ many solutions in the form of $i_0, i_0 + (p-1), \cdots, i_0 + (\frac{q-1}{d} - 1)(p-1)$. Note that j_0 has d choices. This implies that there are $(q-1)$ many elements of D_ℓ mapping into one element in $\mathbb{Z}_p^*$. In a similar manner, we can prove the second multiset equality in the lemma. This completes the whole proof of the lemma. ■

Lemma 6: For $0 \le \ell < q$, we have

$$\{u \pmod{pq} : u \in D_\ell\} = \mathbb{Z}_{pq}^*.$$

Proof: It is obvious that the map from D_ℓ to $\mathbb{Z}_{pq}^*$ with $u \to u \pmod{pq}$ is well-defined. Thus it is sufficient to prove that the map is one-to-one since both D_ℓ and $\mathbb{Z}_{pq}^*$ have the same cardinality.

For $u_1,\ u_2 \in D_\ell$, we write $u_1 = \hat{g}^\ell g^{qi_1} h^{j_1}$ and $u_2 = \hat{g}^\ell g^{qi_2} h^{j_2}$ with $i_1,\ i_2 \in \mathbb{Z}_e$ and $j_1,\ j_2 \in \mathbb{Z}_d$ respectively. Assume that

$$\hat{g}^\ell g^{qi_1} h^{j_1} = u_1 \equiv u_2 = \hat{g}^\ell g^{qi_2} h^{j_2} \pmod{pq}.$$

We will illustrate that $i_1 = i_2$ and $j_1 = j_2$.

Note that

$$g^{qi_1}h^{j_1} = g^{qi_2}h^{j_2} \pmod{pq}$$

as $\gcd(\hat{g}, pq) = 1$. It follows from the CRT that

$$\begin{cases} g^{qi_1+j_1} = g^{qi_2+j_2} \pmod{p}, \\ g^{qi_1} = g^{qi_2} \pmod{q}. \end{cases}$$

This implies that

$$\begin{cases} qi_1 + j_1 \equiv qi_2 + j_2 \pmod{p-1}, \\ qi_1 \equiv qi_2 \pmod{q-1}. \end{cases}$$

Note that $d = \gcd(p-1, q-1)$. It follows from the above equality that

$$\begin{cases} qi_1 + j_1 \equiv qi_2 + j_2 \pmod{d}, \\ qi_1 \equiv qi_2 \pmod{d}. \end{cases}$$

This gives that

$$j_1 \equiv j_2 \pmod{d}.$$

Since j_1 and j_2 belong to $\mathbb{Z}_d$, we have $j_1 = j_2$. In the following, we will show that $i_1 = i_2$ on the basis of the fact that $j_1 = j_2$. Now we have

$$\begin{cases} qi_1 \equiv qi_2 \pmod{p-1}, \\ qi_1 \equiv qi_2 \pmod{q-1}. \end{cases}$$

Since $\gcd(q, p-1) = \gcd(q, q-1) = 1$, it follows that

$$\begin{cases} i_1 \equiv i_2 \pmod{p-1}, \\ i_1 \equiv i_2 \pmod{q-1}. \end{cases}$$

Recall $e = (p-1)(q-1)/d = \text{lcm}(p-1, q-1)$. It follows from the above equations that

$$i_1 = i_2 \pmod{e}.$$

Since i_1 and i_2 belong to $\mathbb{Z}_e$, we have $i_1 = i_2$. This completes the whole proof of the lemma.

■

Lemma 7: Let $\hat{g},\ g \in \mathbb{Z}_{pq^2}^*$ be the same notations as above. For $0 \leq \ell < q$, we have the following multiset equality

$$\{u \pmod{q^2} : u \in D_\ell\} = (p-1) * \hat{\mathfrak{g}}^\ell \langle \mathfrak{g}^q \rangle,$$

where $\hat{\mathfrak{g}}$ and $\mathfrak{g}$ denote $(\hat{g} \pmod{q^2})$ and $(g \pmod{q^2})$, respectively. The set $\hat{\mathfrak{g}}^\ell\langle\mathfrak{g}^q\rangle$ is contained in $\mathbb{Z}_{q^2}^*$ and $(p-1)*\hat{\mathfrak{g}}^\ell\langle\mathfrak{g}^q\rangle$ is the multiset in which each element of $\hat{\mathfrak{g}}^\ell\langle\mathfrak{g}^q\rangle$ appears with multiplicity $p-1$.

Proof: Note that

$$u = \hat{g}^\ell g^{qi} h^j \equiv \hat{\mathfrak{g}}^\ell \mathfrak{g}^{qi} \cdot 1 \equiv \hat{\mathfrak{g}}^\ell (\mathfrak{g}^q)^i \pmod{q^2}.$$

This means that $(u \pmod{q^2})$ belongs to $\hat{\mathfrak{g}}^\ell\langle\mathfrak{g}^q\rangle$ indeed. So the map from D_ℓ to $\hat{\mathfrak{g}}^\ell\langle\mathfrak{g}^q\rangle$ with $u \to u \pmod{q^2}$ is well-defined. Now we count the multiplicity when u runs through the set D_ℓ. Assume that

$$\hat{\mathfrak{g}}^\ell(\mathfrak{g}^q)^i \equiv \hat{\mathfrak{g}}^\ell(\mathfrak{g}^q)^{a_0} \pmod{q^2}$$

for some fixed $a_0 \in \mathbb{Z}_{q-1}$. It follows that

$$qi \equiv qa_0 \pmod{q-1},$$

i.e.,

$$i \equiv a_0 \pmod{q-1}.$$

There exists $\frac{p-1}{d}$ many solutions for $i \in \mathbb{Z}_e$ in the form of $a_0, a_0+(q-1), \cdots, a_0+(\frac{p-1}{d}-1)(q-1)$. Note that $j \in \mathbb{Z}_d$ has d choices. Altogether, there are $(p-1)$ many elements of D_ℓ mapping into one element in $\hat{\mathfrak{g}}^\ell\langle\mathfrak{g}^q\rangle$. This finishes the proof of the lemma.

■

Define $D_\ell(x) = \sum_{u \in D_\ell} x^u \in \mathbb{F}_2[x]$. There exists an important connection between the polynomial $D_\ell(x)$ and the cyclotomic polynomial $\Phi_n(x)$ that will allow us to determine the minimal polynomial of sequences s.

Lemma 8: Let γ be a fixed pq^2-th primitive root of unity and v an element in $\mathbb{Z}_{pq^2}$. Then

$$D_\ell(\gamma^v) = \begin{cases} 1, & \text{if} \quad \gcd(v, pq^2) = q, \\ 0, & \text{if} \quad \gcd(v, pq^2) \in \{p, pq, q^2\} \end{cases}$$

and

$$D_\ell(x) \equiv \begin{cases} 1 & \pmod{\Phi_{pq}(x)}, \\ 0 & \pmod{(\Phi_p(x)\Phi_q(x)\Phi_{q^2}(x))}. \end{cases}$$

Proof: We distinguish two cases according to the distinct value of the greatest common divisor of v and pq^2.

1) For $v \in \mathbb{Z}_{pq^2}$ with $\gcd(v, pq^2) = q$, it follows that γ^v is a pq-th primitive root of unity. On the basis of Lemma 6, we have

$$D_\ell(\gamma^v) = \sum_{u \in D_\ell} \gamma^{uv} = \sum_{u \in \mathbb{Z}_{pq}^*} (\gamma^v)^u.$$

Note that $\sum_{u \in \mathbb{Z}_{pq}^*} \gamma^{uv}$ is equal to the sum of all pq-th primitive roots of unity that is also the coefficient of the second highest term of the cyclotomic polynomial $\Phi_{pq}(x)$. According to Exercise 2.57 of [19], we see that

$$\Phi_{pq}(x) = \frac{\Phi_q(x^p)}{\Phi_q(x)} = \frac{x^{p(q-1)} + x^{p(q-2)} + \cdots + 1}{x^{q-1} + x^{q-2} + \cdots + 1} = x^{(p-1)(q-1)} + 1 \cdot x^{(p-1)(q-1)-1} + \cdots .$$

This indicates that

$$D_\ell(\gamma^v) = \sum_{u \in D_\ell} \gamma^{uv} = \sum_{u \in \mathbb{Z}_{pq}^*} \gamma^{uv} = 1$$

for $v \in \mathbb{Z}_{pq^2}$ with $\gcd(v, pq^2) = q$.

2) For $v \in \mathbb{Z}_{pq^2}$ with $\gcd(v, pq^2) = q^2$, it follows that γ^v is a p-th primitive root of unity. It follows from Lemma 5 and the even parity of $(q-1)$ that

$$\sum_{u \in D_\ell} \gamma^{uv} = (q-1) \sum_{u \in \mathbb{Z}_p^*} (\gamma^v)^u = (q-1) \sum_{u \in \mathbb{Z}_p^*} \gamma^{uv} \equiv 0 \pmod 2.$$

For $v \in \mathbb{Z}_{pq^2}$ with $\gcd(v, pq^2) = pq$ or p, then γ^v is a q-th or q^2-th primitive root of unity respectively. Using the similar argument, it follows from Lemmas 5 and 7 and the even parity of $(p-1)$ that $\sum_{u \in D_\ell} \gamma^{uv} = 0$ in this case.

It follows from the definition of cyclotomic polynomials that

$$D_\ell(x) \equiv \begin{cases} 1 & \pmod{\Phi_{pq}(x)}, \\ 0 & \pmod{\Phi_n(x)} \text{ if } n = p,\ q \text{ or } q^2. \end{cases}$$

Therefore, we get the desired result since the cyclotomic polynomials $\Phi_p(x), \Phi_q(x)$ and $\Phi_{q^2}(x)$ over $\mathbb{F}_2$ are relatively prime. ■

Lemma 9: For $v \in \mathbb{Z}_{pq^2}$, we have

$$\sum_{\ell=0}^{q-1} D_\ell(\gamma^v) = \sum_{u \in \mathbb{Z}_{pq^2}^*} \gamma^{uv} = \begin{cases} 1, & \text{if} \quad \gcd(v, pq^2) = q, \\ 0, & \text{otherwise.} \end{cases}$$

Proof: For $v \in \mathbb{Z}_{pq^2}$ with $\gcd(v, pq^2) = 1$, we see that $\sum_{u \in \mathbb{Z}_{pq^2}^*} \gamma^{uv}$ equals exactly the coefficient of the second highest term of the pq^2-th cyclotomic polynomial $\Phi_{pq^2}(x)$. It follows from the properties of cyclotomic polynomials (see Exercise 2.57 of [19]) that $\Phi_{pq^2}(x) = \Phi_{pq}(x^q)$. This gives the second highest term of the pq^2-th cyclotomic polynomial $\Phi_{pq^2}(x)$ is equal to $zero$ and so $\sum_{u\in\mathbb{Z}^*_{pq^2}} \gamma^{uv} = 0$ for $v \in \mathbb{Z}_{pq^2}$ with $\gcd(v, pq^2) = 1$.

Recall that $\mathbb{Z}^*_{pq^2} = \bigcup_{\ell=0}^{q-1} D_\ell$. For $v \in \mathbb{Z}_{pq^2}$ with $\gcd(v, pq^2) \in \{pq, p, q^2\}$, it follows from Lemma 8 that

$$\sum_{u\in\mathbb{Z}^*_{pq^2}} \gamma^{uv} = \sum_{\ell=0}^{q-1}\sum_{u\in D_\ell} \gamma^{uv} = (q-1)\cdot 0 \equiv 0 \pmod 2.$$

For $v \in \mathbb{Z}_{pq^2}$ with $\gcd(v, pq^2) = q$, it follows that γ^v is a pq-th primitive root of unity. On the basis of Lemma 6, we have

$$\sum_{u\in\mathbb{Z}^*_{pq^2}} \gamma^{uv} = \sum_{\ell=0}^{q-1}\sum_{u\in D_\ell} \gamma^{uv} = \sum_{\ell=0}^{q-1}\sum_{u\in\mathbb{Z}^*_{pq}} \gamma^{uv} = q\sum_{u\in\mathbb{Z}^*_{pq}} \gamma^{uv} = \sum_{u\in\mathbb{Z}^*_{pq}} \gamma^{uv} = 1 \pmod 2.$$

This concludes the whole proof of this lemma. ■

We are now in a position to give a proof of Theorem 1.

Proof of Theorem 1: For $j \in \mathbb{Z}_q$, we denote $\Lambda_j(x) = \sum_{\ell=\frac{q+1}{2}}^{q-1} D_{\ell+j}(x)$, where all the subscripts are understood modulo q here. Note that $\Lambda_0(x) = \sum_{\ell=\frac{q+1}{2}}^{q-1} D_\ell(x)$ is the generating polynomial of the sequence s exactly. Now we claim that $\Lambda_j(\gamma) \neq 0$ for all $j \in \mathbb{Z}_q$.

we first prove $2 \notin D_0$ under the condition that $2^{q-1} \not\equiv 1 \pmod{q^2}$. Suppose that $2 \in D_0$, i.e., $\psi(2) = \frac{2^{\varphi(pq)}-1}{pq} = 0 \pmod{pq}$ according to the definition of Euler quotients. This implies that

$$\frac{2^{\varphi(pq)}-1}{pq} \equiv 0 \pmod q$$

and thus

$$2^{\varphi(pq)} = (2^{q-1})^{p-1} \equiv 1 \pmod{q^2}.$$

This means that the order of $2^{q-1} \pmod{q^2}$ is a factor of $p-1$. However, it follows from $2^{q-1} \not\equiv 1 \pmod{q^2}$ that the order of $2^{q-1} \pmod{q^2}$ is exactly equal to q. This implies that q divides $p-1$, which contradicts the condition that $p < q$. Hence, there exists some fixed nonzero $\sigma \in \mathbb{Z}_q$ such that $2 \in D_\sigma$.

In the following we argue by contradiction. Assume that there exists some $j_0 \in \mathbb{Z}_q$ such that $\Lambda_{j_0}(\gamma) = 0$. By Lemma 4 we get

$$0 = \Lambda_{j_0}(\gamma)^{2^i} = \Lambda_{j_0}(\gamma^{2^i}) = \Lambda_{j_0+i\sigma}(\gamma)$$

for any $i \in \mathbb{Z}_q$. According to $\sigma \neq 0$ in $\mathbb{Z}_q$, the number $j_0 + i\sigma$ runs through $\mathbb{Z}_q$ when i runs through $\mathbb{Z}_q$. This means that $\Lambda_j(\gamma) = 0$ for all $j \in \mathbb{Z}_q$. In particular, we can choose $\Lambda_0(\gamma) = 0$.

For any $v \in D_j$ with $j \in \mathbb{Z}_q$, it follows from Lemma 4 that

$$\Lambda_0(\gamma^v) = \sum_{\ell=\frac{q+1}{2}}^{q-1} D_\ell(\gamma^v) = \sum_{\ell=\frac{q+1}{2}}^{q-1} D_{\ell+j}(\gamma) = \Lambda_j(\gamma) = 0.$$

Note that $\mathbb{Z}_{pq^2}^* = \bigcup_{j=0}^{q-1} D_j$. It is immediate that $\Lambda_0(\gamma^v) = 0$ for any $v \in \mathbb{Z}_{pq^2}^*$. Thus the cyclotomic polynomial $\Phi_{pq^2}(x)$ divides $\Lambda_0(x)$. By Lemma 8, we see that $\Phi_{q^2}(x)$ divides $\Lambda_0(x)$. Then $\Phi_{pq^2}(x)\Phi_{q^2}(x)$ divides $\Lambda_0(x)$ since $\gcd(\Phi_{pq^2}(x), \Phi_{q^2}(x)) = 1$. On the basis of Exercise 2.57 of [19], we have

$$\Phi_{pq^2}(x)\Phi_{q^2}(x) = \Phi_{q^2}(x^p) = \Phi_q(x^{pq}) = \sum_{j=0}^{q-1} x^{jpq}.$$

We write

$$\Lambda_0(x) \equiv \Phi_{q^2}(x^p)\pi(x) \pmod{x^{pq^2} - 1}.$$

Note that

$$x^{pq}\Phi_q(x^{pq}) = x^{pq}\sum_{j=0}^{q-1} x^{jpq} \equiv \sum_{j=0}^{q-1} x^{jpq} \equiv \Phi_q(x^{pq}) \pmod{x^{pq^2} - 1}.$$

We can restrict $\deg \pi(x) < pq$ and thus $\pi(x)$ can be written as $\pi(x) = \sum_{i=0}^{t-1} x^{\nu_i}$, where $0 \leq \nu_0 < \nu_1 < \cdots < \nu_{t-1} < pq$. Then

$$\Lambda_0(x) \equiv \pi(x)\Phi_q(x^{pq}) \equiv \sum_{i=0}^{t-1} x^{\nu_i} \sum_{j=0}^{q-1} x^{jpq} \equiv \sum_{i=0}^{t-1}\sum_{j=0}^{q-1} x^{\nu_i + jpq} \pmod{x^{pq^2} - 1}.$$

However $\Lambda_0(x)$ has $\frac{1}{2}(p-1)(q-1)^2$ terms and $\sum_{i=0}^{t-1}\sum_{j=0}^{q-1} x^{\nu_i+jpq}$ has qt terms, which is a contradiction since the prime q does not divide $\frac{1}{2}(p-1)(q-1)^2$. It follows that $\Lambda_j(\gamma) \neq 0$ for any $j \in \mathbb{Z}_q$.

This implies that $\Lambda_j(\gamma^\nu) \neq 0$ for all $\nu \in \mathbb{Z}_{pq^2}^*$ and $0 \leq j < q$. In particular, we have $\Lambda_0(\gamma^\nu) \neq 0$ for all $\nu \in \mathbb{Z}_{pq^2}^*$. By Lemma 8, for $\nu \in \mathbb{Z}_{pq^2}$ and $0 \leq j < q$ we get

$$\Lambda_0(\gamma^\nu) = \begin{cases} 0, & \text{if} \quad \gcd(\nu, pq^2) \in \{p, pq, q^2, pq^2\}, \\ \frac{q-1}{2}, & \text{if} \quad \gcd(\nu, pq^2) = q. \end{cases}$$

This implies that $(x-1)(\Phi_p(x)\Phi_q(x)\Phi_{q^2}(x))$ divides $\Lambda_0(x)$ if $q \equiv 3 \pmod 4$. Hence the minimal polynomial for the case of $q \equiv 3 \pmod 4$ is

$$M_{\mathbf{s}}(x) = \frac{x^{pq^2}-1}{(x-1)\Phi_p(x)\Phi_q(x)\Phi_{q^2}(x)} = \Phi_{pq^2}(x)\Phi_{pq}(x)$$

by using the basic properties of cyclotomic polynomials. In a similar manner, if $q \equiv 1 \pmod 4$, then $\Phi_{pq}(x)$ divides $\Lambda_0(x)$. This yields that the minimal polynomial for the case of $q \equiv 1 \pmod 4$ is

$$M_{\mathbf{s}}(x) = \frac{x^{pq^2}-1}{(x-1)(\Phi_p(x)\Phi_q(x)\Phi_{pq}(x))\Phi_{q^2}(x))} = \Phi_{pq^2}(x).$$

Note that the linear complexity of s is equal to the degree of the minimal polynomial of the sequence and so the third assertion in Theorem 1 follows. This completes the whole proof of Theorem 1.

In the following, we will give a small example for confirming our main results.

Example 1: Let $p = 3$ and $q = 7$. The least period of the binary threshold sequence s derived from modulo pq is 147. The sequence s in one period is

$$\{0,0,0,0,1,1,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,1,1,0,1,1,0,0,0,0,0,0,0,1,0,0,0,0,0,1,$$
$$1,0,0,1,0,1,0,0,0,0,0,1,1,0,0,0,0,1,0,0,0,0,0,1,0,0,0,0,0,0,1,0,1,1,0,1,0,0,0,0,0,$$
$$0,1,0,0,0,0,0,1,0,0,0,0,1,1,0,0,0,0,0,1,0,1,0,0,1,1,0,0,0,0,0,1,0,0,0,0,0,0,0,0,1,1,$$
$$0,1,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,1,1,0,0,0\}.$$

The minimal polynomial of the sequence s over $\mathbb{F}_2$ is

$$\begin{aligned} &x^{96}+x^{95}+x^{93}+x^{92}+x^{90}+x^{89}+x^{87}+x^{86}+x^{84}+x^{83}+x^{81}+x^{80}+x^{78}+x^{77}+x^{75}\\ &+x^{74}+x^{72}+x^{71}+x^{69}+x^{68}+x^{66}+x^{65}+x^{63}+x^{62}+x^{60}+x^{59}+x^{57}+x^{56}+x^{54}\\ &+x^{53}+x^{51}+x^{50}+x^{48}+x^{46}+x^{45}+x^{43}+x^{42}+x^{40}+x^{39}+x^{37}+x^{36}+x^{34}+x^{33}\\ &+x^{31}+x^{30}+x^{28}+x^{27}+x^{25}+x^{24}+x^{22}+x^{21}+x^{19}+x^{18}+x^{16}+x^{15}+x^{13}+x^{12}\\ &+x^{10}+x^{9}+x^{7}+x^{6}+x^{4}+x^{3}+x+1 \end{aligned}$$

and the linear complexity of this sequence is $(p-1)\cdot(q^2-1) = 2\cdot 48 = 96$.

III. Conclusion Remarks

In this paper, we determined the linear complexities of a class of binary sequences with period pq^2 on basis of the Euler quotients modulo pq. In addition, the proposed sequences have a good balance asymptotically if the prime p tends to infinity, i.e., the number of 1's is asymptotically equal to the number of 0's in one period if p tends to infinity. Finally, there are several unsolved problems about the proposed sequences. For example, it is not known whether this family of sequences derived from the Euler quotient modulo pq can induce more optimal families of perfect polyphase sequences similar to [23]. Another interesting problem is to study k-error linear complexities of the proposed sequences.

Acknowledgment

The work of Chang-An Zhao is partially supported by National Key R&D Program of China under Grant No. 2017YFB0802500 and by NSFC under Grant No. 61472457. The work of Shuhong Gao was partially supported by the National Science Foundation under grants DMS-1403062 and DMS-1547399. Part of the work were done while the first and third authors were Visiting Scholars at Clemson University.

References

[1] T. Agoh, K. Dilcher, and L. Skula, "Fermat quotients for composite moduli," *Journal of Number Theory*, vol. 66, no. 1, pp. 29–50, 1997.

[2] E. Bai, X. Liu, and G. Xiao, "Linear complexity of new generalized cyclotomic sequences of order two of length pq," *IEEE Transactions on Information Theory*, vol. 51, no. 5, pp. 1849–1853, May 2005.

[3] Z. Chen, "Trace representation and linear complexity of binary sequences derived from Fermat quotients," *Sci. China Inform. Sci.*, vol. 57, no. 11, pp. 1–10, 2014.

[4] Z. Chen, X. Du, and R. Marzouk, "Trace representation of pseudorandom binary sequences derived from Euler quotients," *Appli. Alg. Eng. Commun. Comp.*, vol. 26, no. 6, pp. 555–570, 2015.

[5] Z. Chen, Z. Niu, and C. Wu, "On the k-error linear complexity of binary sequences derived from polynomial quotients," *Sci. China Inform. Sci.*, vol. 58, no. 9, pp. 1–15, 2015.

[6] Z. Chen and A. Winterhof, "Additive character sums of polynomial quotients," *Contemp Math.*, vol. 579, pp. 67–73, 2012.

[7] ——, "On the distribution of pseudorandom numbers and vectors derived from Euler-Fermat quotients," *Int J. Number Theory*, vol. 8, pp. 631–641, 2012.

[8] Z. Chen and X. Du, "On the linear complexity of binary threshold sequences derived from Fermat quotients," *Designs, Codes and Cryptography*, vol. 67, no. 3, pp. 317–323, 2013.

[9] Z. Chen, V. Edemskiy, P. Ke, and C. Wu, "On k-error linear complexity of pseudorandom binary sequences derived from Euler quotients," *Advances in Mathematics of Communications*, vol. 12, no. 4, pp. 805–816, 2018.

[10] Z. Chen, Z. Niu, and C. Wu, "On the k-error linear complexity of binary sequences derived from polynomial quotients," *Sci. China Inform. Sci.*, vol. 58, no. 9, pp. 1–15, 2015.

[11] Z. Chen, A. Ostafe, and A. Winterhof, "Structure of pseudorandom numbers derived from fermat quotients," in *Arithmetic of Finite Fields*, M. A. Hasan and T. Helleseth, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 73–85.

[12] C. Ding, G. Xiao, and W. Shan, *The Stability Theory of Stream Ciphers*. Springer, Berlin-Verlag, 1991.

[13] C. Ding and T. Helleseth, "New generalized cyclotomy and its applications," *Finite Fields and Their Applications*, vol. 4, no. 2, pp. 140 – 166, 1998. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1071579798902076

[14] P. Dingyi, S. Arto, and D. Cunsheng, *Chinese remainder theorem: applications in computing, coding, cryptography*. World Scientific, 1996.

[15] P. Fan and M. Darnell, *Sequence design for communications applications*. Australia and New Zealand: Jacaranda Wiley Ltd, 1996.

[16] S. W. Golomb and G. Gong, *Signal Design for Good Correlation for Wireless Communication,Cryptography and Radar*. Cambridge University Press, 2005.

[17] L. Hu, Q. Yue, and M. Wang, "The linear complexity of whiteman's generalized cyclotomic sequences of period$p^{m+1}q^{n+1}$," *IEEE Transactions on Information Theory*, vol. 58, no. 8, pp. 5534–5543, Aug 2012.

[18] Y. Jiang and D. Lin, "Lower and upper bounds on the density of irreducible NFSRs," *IEEE Trans. Inform. Theory*, vol. 64, no. 5, pp. 3944–3952, 2018.

[19] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*. New York, NY, USA: Cambridge University Press, 1986.

[20] J. Massey, "Shift-register synthesis and bch decoding," *IEEE Transactions on Information Theory*, vol. 15, no. 1, pp. 122–127, January 1969.

[21] A. Michael, *Algebra*. Pearson Prentice Hall, 2011.

[22] Z. Niu, Z. Chen, and X. Du, "Linear complexity problems of level sequences of Euler quotients and their related binary sequences," *Sci. China Inform. Sci.*, vol. 59, pp. 1–12, 2016.

[23] K. Park, H. Song, D. S. Kim, and S. W. Golomb, "Optimal families of perfect polyphase sequences from the array structure of fermat-quotient sequences," *IEEE Transactions on Information Theory*, vol. 62, no. 2, pp. 1076–1086, Feb 2016.

[24] W. Su, Y. Yang, Z. Zhou, and X. Tang, "New quaternary sequences of even length with optimal auto-correlation," *Sci. China Inform. Sci.*, vol. 61, no. 2, pp. 1–13, 2018.

[25] Y. Yang and X. Tang, "Generic construction of binary sequences of period 2n with optimal odd correlation magnitude based on quaternary sequences of odd period N," *IEEE Trans. Information Theory*, vol. 64, no. 1, pp. 384–392, 2018.

[26] J. Zhang, T. Tian, W. Qi, and Q. Zheng, "A new method for finding affine sub-families of NFSR sequences," *IEEE Trans. Inform. Theory*, vol. 65, no. 2, pp. 1249–1257, 2019.

[27] X.-X. Zhao, T. Tian, and W.-F. Qi, "A ring-like cascade connection and a class of NFSRs with the same cycle structures," *Designs, Codes and Cryptography*, vol. 86, no. 12, pp. 2775–2790, 2018.