The Linear Complexity of Whiteman's Generalized Cyclotomic Sequences of Period $p^{m+1}q^{n+1}$

Liqin Hu, Qin Yue, and Minhong Wang, *Member, IEEE*

***Abstract*—In this paper, we mainly get three results. First, let p, q be distinct primes with $\gcd((p-1)p,(q-1)q) = \gcd(p-1,q-1) = e$; we give a method to compute the linear complexity of Whiteman's generalized cyclotomic sequences of period $p^{m+1}q^{n+1}$. Second, if $e=4$, we compute the exact linear complexity of Whiteman's generalized cyclotomic sequences. Third, if $p \equiv q \equiv 5 \pmod 8$, $\gcd(p-1,q-1)=4$, and we fix a common primitive root g of both p and q, then $2 \in H_0 = (g)$, which is a subgroup of the multiplicative group Z_{pq}^*, if and only if Whiteman's generalized cyclotomic numbers of order 4 depend on the decomposition $pq = a^2+4b^2$ with $4|b$.**

***Index Terms*—Generalized cyclotomic number, linear complexity.**

I. Introduction

PSEUDORANDOM sequences have wide applications in simulation, software testing, radar systems, stream ciphers, and so on. Several authors show cyclotomic sequences with good randomness properties [2], [8], [9], [12]. Although Whiteman [15] studied the generalized cyclotomy of order 2 and 4 for the purpose of searching for residue difference sets, several authors apply generalized cyclotomy to construct cyclotomic sequences (see [1], [3]–[7], and [14]).

A sequence $s=(s_0,s_1,\ldots,s_{N-1},\ldots)$ is said to be *N-periodic* if $s_i = s_{i+N}$ for all $i \geq 0$. The linear complexity of a sequence s over $GF(2)$ is an important characteristic of its equality (see [11]). It is defined to be the smallest positive integer L for which there exist constants $c_1,\ldots,c_L \in GF(2)$ such that

$$s_g = c_1 s_{g-1} + c_2 s_{g-2} + \cdots + c_L s_{g-L} \text{ for all } g \geq L.$$

In this paper, generalized cyclotomic sequences always mean Whiteman's generalized cyclotomic sequences. We will calculate the linear complexity of generalized cyclotomic sequences of period $N = p^{m+1}q^{n+1} (m,n \geq 0)$. Let us recall the construction rules of these generalized cyclotomic sequences.

In this paper, we always assume that p and q are distinct odd primes and $N = p^{m+1}q^{n+1}, m,n \geq 0$, unless otherwise stated.

Manuscript received May 27, 2011; revised November 03, 2011 and February 21, 2012; accepted April 16, 2012. Date of publication April 24, 2012; date of current version July 10, 2012. This work was supported in part by the National Natural Science Foundation of China under Grants 11171150 and 10971250.

L. Hu and Q. Yue are with the Department of Mathematics, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China (e-mail: huqin0916@126.com; yueqin@nuaa.edu.cn).

M. Wang is with the Faculty of Education, The University of Hong Kong, Pokfulam, Hong Kong (e-mail: magwang@hku.hk).

Communicated by M. G. Parker, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2012.2196254

Let $\gcd((p-1)p^m,(q-1)q^n) = \gcd(p-1,q-1) = e$ and $R = \frac{(p-1)(q-1)}{e}$. Although N does not possess a primitive root, by the Chinese remainder theorem there exists a common primitive root g of both p^{m+1} and q^{n+1}.

We have two relations (see [9])

$$Z_{p^{m+1}} = \bigcup_{i=0}^{m+1} p^i Z_{p^{m+1}}^*, \quad Z_{q^{n+1}} = \bigcup_{i=0}^{n+1} q^i Z_{q^{n+1}}^*$$

where $p^{m+1}Z_{p^{m+1}}^* = \{0\}$ and $q^{n+1}Z_{q^{n+1}}^* = \{0\}$.

Now we investigate a factorization of Z_N. Let $d := \mathrm{ord}_N(g)$ denote the multiplicative order of g modulo N; then

$$d = \mathrm{ord}_N(g) = \mathrm{lcm}(\mathrm{ord}_{p^{m+1}}(g), \quad \mathrm{ord}_{q^{n+1}}(g)) = \frac{(p-1)(q-1)p^m q^n}{e}.$$

Then, the subgroup $D_0 = (g)$ of the multiplicative group Z_N^* is of order d.

Let y be an integer satisfying the simultaneous congruences

$$y \equiv g \pmod{p^{m+1}}, \; y \equiv 1 \pmod{q^{n+1}}. \tag{1.1}$$

We define generalized cyclotomic classes analogous to [15]

$$D_k = \{g^s y^k : s = 0,1,\ldots,d-1\}, \; k = 0,1,\ldots,e-1. \tag{1.2}$$

Then, we get

$$Z_N^* = \bigcup_{k=0}^{e-1} D_k.$$

Lemma 1.1:

$$Z_N = \bigcup_{i=0}^{m+1}\bigcup_{j=0}^{n+1} p^i q^j Z_N^* \tag{1.3}$$

where the multiplication is performed in the ring Z_N and $p^{m+1}q^{n+1}Z_N^* = \{0\}$.

Proof: It is clear from [5, Lemma 12]. □

If $i \leq m, \; j \leq n$, then

$$p^i q^j D_k = \{p^i q^j a | a \in D_k\}, \quad k = 0,\ldots,d-1.$$

Hence

$$Z_N = \bigcup_{i=0}^{m}\bigcup_{j=0}^{n}\bigcup_{k=0}^{e-1} p^i q^j D_k \bigcup_{i=0}^{m} p^i q^{n+1} Z_N^* \bigcup_{j=0}^{n+1} p^{m+1} q^j Z_N^*. \tag{1.4}$$

For convenience, we give a definition.

Definition 1.2: The assumptions are as above. Define subsets of Z_N

$$D_k^{(i,j)} = \begin{cases} p^i q^j D_k, & \text{if } i \le m, j \le n, 0 \le k \le e-1 \\ p^i q^{n+1} Z_N^*, & \text{if } i \le m, j = n+1, k = 0 \\ p^{m+1} q^j Z_N^*, & \text{if } i = m+1, j \le n, k = 0 \\ \{0\}, & \text{if } i = m+1, j = n+1, k = 0. \end{cases}$$

So $D_0^{(i,n+1)} = p^i q^{n+1} Z_N^*$ for $i \le m$, $D_0^{(m+1,j)} = p^{m+1} q^j Z_N^*$ for $j \le n$, and $D_0^{(m+1,n+1)} = \{0\}$, and index sets for $0 \le i \le m+1$ and $0 \le j \le n+1$ are given as

$$I_{i,j} \subset \begin{cases} \{0,1,\cdots,e-1\}, & \text{if } i \le m, j \le n \\ \{0\}, & \text{otherwise.} \end{cases}$$

Suppose that $\Omega = \bigcup_{i=0}^{m+1} \bigcup_{j=0}^{n+1} \bigcup_{k \in I_{i,j}} D_k^{(i,j)}$. We can define the generalized cyclotomic binary sequence s of period N as

$$s_i = \begin{cases} 1, & \text{if } i \pmod N \in \Omega, \\ 0, & \text{otherwise,} \end{cases} \quad \text{for all } i \ge 0. \tag{1.5}$$

Define

$$s(x) = s_0 + s_1 x + \cdots + s_{N-1} x^{N-1} = \sum_{i \in \Omega} x^i \tag{1.6}$$

as the characteristic polynomial of the sequence s. It is well known that the minimal polynomial of the binary sequence s of period N is given by

$$m(x) = \frac{x^N - 1}{\gcd(x^N - 1, s(x))}$$

and that the linear complexity of s is given by

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

In this paper, there are three main results. First, we show a method to compute the linear complexity of the aforementioned generalized cyclotomic sequences of period $p^{m+1}q^{n+1}$. Second, if $\gcd(p^m(p-1), q^n(q-1)) = e = 4$, we easily calculate the linear complexity of the aforementioned generalized cyclotomic sequences. Third, if $p \equiv q \equiv 5 \pmod 8$, $\gcd(p-1, q-1) = 4$, and we fix a common primitive root g of both p and q, then $2 \in H_0 = (g)$, which is a subgroup of the multiplicative group Z_{pq}^*, if and only if Whiteman's generalized cyclotomic numbers of order 4 depend on the decomposition $pq = a^2 + 4b^2$ with $4|b$.

II. Generalized Cyclotomic Sequences of Period $p^{m+1}q^{n+1}$

In this section, we generalize the results from [9] and give a formula for the linear complexity of the generalized cyclotomic binary sequence s of period $N = p^{m+1}q^{n+1}$ defined as (1.5).

Lemma 2.1:

1) Let $e = \gcd(p-1, q-1)$ and $R = \frac{(p-1)(q-1)}{e}$; then

$$D_0 = \{g^k + hpq | k = 0,1,\ldots,R-1; h = 0,1,\cdots,p^m q^n - 1\}.$$

If $i \le m$ and $j \le n$, then see the first equation shown at the bottom of the page.

2) If $i \le m$ and $j = n+1$, then see the second equation shown at the bottom of the page.
3) If $i = m+1$ and $j \le n$, then see the third equation shown at the bottom of the page.

Proof:

1) Since g is a common primitive root of both p^{m+1} and q^{n+1}, g is also a common primitive root of both p and q. Hence in the multiplicative group Z_{pq}^*, $\mathrm{ord}_{pq}(g) = (p-1)(q-1)/e = R$, so $g^k \not\equiv g^{k'} \pmod{pq}$ for $0 \le k \ne k' \le R-1$.
If $a \equiv g^k \pmod{pq}$ for $0 \le k \le R-1$, then $p \nmid a$ and $q \nmid a$, so $a \in Z_N^*$. Suppose that $a \in D_r$, where $r \in \{0,1,\ldots,e-1\}$; then $a \equiv y^r g^{k_1} \pmod{p^{m+1}q^{n+1}}$. So $a \equiv y^r g^{k_1} \equiv g^{r+k_1} \pmod p$ and $a \equiv g^{k_1} \pmod q$. Hence, $p-1 | r + k_1 - k$ and $q - 1 | k_1 - k$. Then by $\gcd(p-1, q-1) = e$, $e|r$, so $r = 0$ and $a \in D_0$.
Moreover, if $(k,h) \ne (k',h')$ for $0 \le k, k' \le R-1$ and $0 \le h, h' \le p^m q^n - 1$, then $g^k + hpq \not\equiv g^{k'} + h'pq \pmod{p^{m+1}q^{n+1}}$. By $|D_0| = p^m q^n (p-1)(q-1)/e$, this proves the first part of 1). Similarly, we can prove the second part of 1).

$$D_0^{(i,j)} = p^i q^j D_0 = \{p^i q^j (g^k + hpq) | k = 0,1,\cdots,R-1; h = 0,1,\ldots,p^{m-i}q^{n-j} - 1\}$$

$$D_0^{(i,n+1)} = p^i q^{n+1} Z_N^* = \{p^i q^{n+1}(g^k + hp) | k = 0,1,\cdots,p-2, h = 0,1,\ldots,p^{m-i} - 1\}$$

$$D_0^{(m+1,j)} = p^{m+1} q^j Z_N^* = \{p^{m+1} q^j (g^k + hq) | k = 0,1,\cdots,q-2, h = 0,1,\ldots,q^{n-j} - 1\}$$

2) Since $\eta : p^i q^{n+1} Z_N^* \rightarrow p^i Z_{p^{m+1}}^* \times \{0\}$ is a bijective map and by [9] $p^i Z_{p^{m+1}}^* = \{p^i(g^k + hp) | k = 0, 1, \ldots, p-2, h = 0, 1, \ldots, p^{m-i}-1\}$, we prove 2). Similarly, we can prove 3). □

Let α be a primitive Nth root of unity in an extension of $GF(2)$. Then by Blahut's theorem, the linear complexity of the sequence s defined as (1.5) is

$$L = N - |\{t | s(\alpha^t) = 0, t = 0, 1, \ldots, N-1\}| \tag{2.1}$$

where $s(x) = s_0 + s_1 x + \cdots + s_{N-1} x^{N-1}$ is the characteristic polynomial of the sequence s. So the linear complexity of the sequence s reduces to counting the number of roots of $s(x)$ in the set $\{\alpha^t | t = 0, 1, \ldots, N-1\}$.

To explore the roots of the polynomial $s(x)$, we need the following auxiliary polynomials for $i \le m, j \le n$

$$s_{i,j}(x) = \sum_{l \in D_0^{(i,j)}} x^l = \sum_{k=0}^{R-1} x^{p^i q^j g^k} \sum_{h=0}^{p^{m-i} q^{n-j} - 1} x^{p^{i+1} q^{j+1} h} \tag{2.2}$$

$$s_{i,n+1}(x) = \sum_{l \in D_0^{(i,n+1)}} x^l = \sum_{k=0}^{p-2} x^{p^i q^{n+1} g^k} \sum_{h=0}^{p^{m-i}-1} x^{p^{i+1} q^{n+1} h}$$

$$s_{m+1,j}(x) = \sum_{l \in D_0^{(m+1,j)}} x^l = \sum_{k=0}^{q-2} x^{p^{m+1} q^j g^k} \sum_{h=0}^{q^{n-j}-1} x^{p^{m+1} q^{j+1} h}.$$

Since $D_k^{(i,j)} = y^k D_0^{(i,j)}$ for $i \le m$ and $j \le n$, by the definition of s as (1.5)

$$s(\alpha^t) = \sum_{i=0}^{m} \sum_{j=0}^{n} \sum_{k \in I_{i,j}} s_{i,j}(\alpha^{y^k t}) + \sum_{i=0}^{m} \delta_{i,n+1} s_{i,n+1}(\alpha^t) + \sum_{j=0}^{n+1} \delta_{m+1,j} s_{m+1,j}(\alpha^t) \tag{2.3}$$

where $\sum_{k \in I_{i,j}} s_{i,j}(\alpha^{y^k t}) = 0$ if $I_{i,j} = \emptyset$, $i \le m, j \le n$, and for $i \le m$ and $j \le n+1$,

$$\delta_{i,n+1} = \begin{cases} 1, & \text{if } I_{i,n+1} = \{0\}, \\ 0, & \text{if } I_{i,n+1} = \emptyset, \end{cases} \quad \delta_{m+1,j} = \begin{cases} 1, & \text{if } I_{m+1,j} = \{0\} \\ 0, & \text{if } I_{m+1,j} = \emptyset. \end{cases} \tag{2.4}$$

Lemma 2.2: For integers h and t, we have equalities

$$s_{i,j}(\alpha^{tg^h}) = s_{i,j}(\alpha^t), i \le m+1, j \le n+1.$$

Proof: Since $g^h D_0^{(i,j)} = D_0^{(i,j)}$ for $i \le m+1$ and $j \le n+1$, we prove Lemma 2.2. □

Lemma 2.3: Let $p \nmid t$ and $q \nmid t$. Suppose that $i \le m, j \le n$, and $i + j \le m + n - 1$. Then, $s_{i,j}(\alpha^t) = 0$.

Proof: Since α is a $p^{m+1} q^{n+1}$th primitive root of unity, we have

$$0 = \alpha^{p^{m+1} q^{n+1}} - 1 = (\alpha^{p^i q^j} - 1)(1 + \alpha^{p^i q^j} + \alpha^{2p^i q^j} + \cdots + \alpha^{(p^{m+1-i} q^{n+1-j} - 1) p^i q^j})$$

for $i + j \le m + n + 1$. Hence

$$\sum_{h=0}^{p^{m+1-i} q^{n+1-j} - 1} \alpha^{h p^i q^j} = 0. \tag{2.5}$$

Since $p \nmid t$ and $q \nmid t$, α^t is also a $p^{m+1} q^{n+1}$th primitive root of unity. If $i \le m, j \le n$, and $i+j \le m+n-1$, then by (2.2) and (2.5), $s_{i,j}(\alpha^t) = \sum_{k=0}^{R-1} \alpha^{tp^i q^j g^k} \sum_{h=0}^{p^{m-i} q^{n-j} - 1} \alpha^{tp^{i+1} q^{j+1} h} = 0$. □

Lemma 2.4: Let $p \nmid t$, $q \nmid t$, $0 \le u \le m+1$, and $0 \le v \le n+1$.

1) Suppose that $i \le m$, $j \le n$; then

$$s_{i,j}(\alpha^{tp^u q^v}) = \begin{cases} 0, & \text{if either } u < m-i \text{ or } v < n-j \\ s_{m,n}(\alpha^t), & \text{if } u = m-i, v = n-j \\ (q-1)/e, & \text{if } u = m-i, v > n-j \\ (p-1)/e, & \text{if } u > m-i, v = n-j \\ 0, & \text{if } u > m-i, v > n-j. \end{cases}$$

2) Suppose that $i \le m$, $j = n+1$; then

$$s_{i,n+1}(\alpha^{tp^u q^v}) = \begin{cases} 1, & \text{if } u = m-i \\ 0, & \text{if } u \ne m-i. \end{cases}$$

3) Suppose that $i = m+1$, $j \le n$, then

$$s_{m+1,j}(\alpha^{tp^u q^v}) = \begin{cases} 1 & \text{if } v = n-j \\ 0, & \text{if } v \ne n-j. \end{cases}$$

Proof:

1) Suppose that $i \le m$, $j \le n$, if $u < m-i$. Without loss of generality, we assume that $v < n-j$; then for any $b \in \{0, 1, \ldots, p^{m-u-i} q^{n-v-j} - 1\}$, there exist $p^u q^v$ elements $h \in \{0, 1, \ldots, p^{m-i} q^{m-j} - 1\}$ such that $b \equiv h \pmod{p^{m-u-i} q^{n-v-j}}$. Hence by (2.2) and (2.5)

$$\begin{aligned} & s_{i,j}(\alpha^{tp^u q^v}) \\ & = p^u q^v \sum_{k=0}^{R-1} \alpha^{tp^{u+i} q^{v+j} g^k} \sum_{b=0}^{p^{m-i-u} q^{n-j-v} - 1} \alpha^{tp^{i+u+1} q^{j+v+1} b} \\ & = 0. \end{aligned}$$

Similarly, if $u < m-i$ and $v \ge n-j$, then we get the same result.

If $u = m-i$ and $v = n-j$, then by (2.2) and $\alpha^{p^{u+i+1} q^{v+j+1}} = 1$, $s_{i,j}(\alpha^{tp^u q^v}) \equiv s_{m,n}(\alpha^t) \pmod 2$.

If $u = m-i$ and $v > n-j$, then $\alpha^{p^{u+i+1} q^{v+j+1}} = 1$ and $\beta = \alpha^{p^{i+u} q^{v+j}}$ is a pth primitive root of unity. For any $c \in \{1, \ldots, p-1\}$, there are $(q-1)/e$ elements $g^k \in \{g^k | k = 0, 1, \ldots, R-1\}$ such that $c \equiv g^k \pmod p$.

Hence by (2.2) and (2.5), $s_{i,j}(\alpha^{tp^up^v}) = p^{m-i}q^{n-j}(q-1)/e\sum_{c=1}^{p-1}\beta^{tc} \equiv (q-1)/e \pmod 2$. Similarly, if $u > m-i$ and $v = n-j$, then $s_{i,j}(\alpha^{tp^up^v}) \equiv (p-1)/e \pmod 2$.

If $u > m-i, v > n-j$, then by (2.2) and $\alpha^{p^{u+i}q^{v+j}} = 1$, $s_{i,j}(\alpha^{p^uq^vt}) = Rp^{m-i}q^{n-j} \equiv R \equiv 0 \pmod 2$.

2) Suppose that $i \le m$ and $j = n+1$. If $u > m-i$, then by (2.2) and $\alpha^{tp^{u+i}q^{v+n+1}} = 1$, $s_{i,n+1}(\alpha^{tp^uq^v}) = (p-1)p^{m-i} \equiv 0 \pmod 2$.

If $u = m-i$, then $\alpha^{p^{u+i+1}q^{v+n+1}} = 1$ and $\alpha^{p^{u+i}q^{v+n+1}}$ is a pth primitive root of unity. Hence by (2.2) and (2.5), $s_{i,n+1}(\alpha^{tp^uq^v}) = p^{m-i}\sum_{k=0}^{p-2}\alpha^{tp^{u+i}q^{v+n+1}g^k} \equiv 1 \pmod 2$.

If $u < m-i$, then for any $b \in \{0,1,\ldots,p^{m-u-i}-1\}$, there exist p^u elements $h \in \{0,1,\ldots,p^{m-i}-1\}$ such that $b \equiv h \pmod{p^{m-i-u}}$. Hence by (2.2) and (2.5), $s_{i,n+1}(\alpha^{tp^uq^v}) = p^u\sum_{k=0}^{p-2}\alpha^{tp^{u+i}q^{v+n+1}g^k}\sum_{b=0}^{p^{m-u-i}-1}\alpha^{tp^{u+i+1}q^{v+n+1}b} = 0$.

3) The proof is similar to that for (2). □

By the previous lemmas, we know that the computation of the linear complexity of the sequence s turns into the computation of the values of $s_{m,n}(x)$ for the generalized cyclotomic sequence.

We know that g is also a common primitive root of both p and q. Let $H_0 = (g)$ be a subgroup of the multiplicative group Z_{pq}^*. Let us introduce the polynomial $T(x) = \sum_{l\in H_0}x^l$.

Let $\beta = \alpha^{p^mq^n}$ be a pqth primitive root of unity in an extension field of $GF(2)$. Then we have $s_{m,n}(\alpha^t) = T(\beta^t)$.

For the computation of the linear complexity of the sequence s defined as (1.5), we need the following notations. For $0 \le u \le m$ and $0 \le v \le n$, set

$$E_{u,v} = |\{k| \sum_{l\in I_{u,v}} T(\beta^{y^{k+l}}) = 0, k = 0,1,\ldots,e-1\}|$$
$$F_{u,v} = |\{k| \sum_{l\in I_{u,v}} T(\beta^{y^{k+l}}) = 1, k = 0,1,\ldots,e-1\}|.$$

Set for $0 \le u \le m$ and $0 \le v \le n$

$$\sigma_{u,v} = \frac{q-1}{e}\sum_{j=v+1}^{n}|I_{u,j}| + \frac{p-1}{e}\sum_{i=u+1}^{m}|I_{i,v}| + \delta_{u,n+1} + \delta_{m+1,v} + \delta_{m+1,n+1} \quad (2.6)$$
$$\sigma_{u,n+1} = \frac{q-1}{e}\sum_{j=0}^{n}|I_{u,j}| + \delta_{u,n+1} + \delta_{m+1,n+1}$$
$$\sigma_{m+1,v} = \frac{p-1}{e}\sum_{i=0}^{m}|I_{i,v}| + \delta_{m+1,v} + \delta_{m+1,n+1}$$

where $\delta_{u,n+1}$, $\delta_{m+1,v}$, $\delta_{m+1,n+1}$ are defined as (2.4) and $\sum_{j=v+1}^{n}|I_{u,j}| = 0$ if $v = n$. Set

$$A_{u,v} = \begin{cases} E_{u,v}, & \text{if } \sigma_{u,v} \equiv 0 \pmod 2 \\ F_{u,v}, & \text{if } \sigma_{u,v} \equiv 1 \pmod 2 \end{cases}$$
$$A_{u,n+1} = \begin{cases} 1, & \text{if } \sigma_{u,n+1} \equiv 0 \pmod 2 \\ 0, & \text{if } \sigma_{u,n+1} \equiv 1 \pmod 2 \end{cases}$$
$$A_{m+1,v} = \begin{cases} 1, & \text{if } \sigma_{m+1,v} \equiv 0 \pmod 2 \\ 0, & \text{if } \sigma_{m+1,v} \equiv 1 \pmod 2. \end{cases}$$

Now we get the most important theorem in this section.

Theorem 2.5: If the sequence s is defined as (1.5), then the linear complexity of the sequence s is

$$L = p^{m+1}q^{n+1} - \sum_{u=0}^{m}\sum_{v=0}^{n}A_{u,v}p^uq^vR - \sum_{u=0}^{m}A_{u,n+1}p^u(p-1) - \sum_{v=0}^{n}A_{m+1,v}q^v(q-1) - \delta$$

where

$$\delta = \begin{cases} 0, & \text{if } I_{m+1,n+1} = \{0\} \\ 1, & \text{if } I_{m+1,n+1} = \emptyset. \end{cases} \quad (2.7)$$

Proof: If any $t = p^uq^vy^kg^h \in D_k^{(u,v)}$ for $0 \le u \le m+1$, $0 \le v \le n+1$ and $0 \le k \le e-1$, then by Lemma 2.2 and (2.2)

$$s(\alpha^{p^uq^vy^kg^h}) = \sum_{i=0}^{m}\sum_{j=0}^{n}\sum_{l\in I_{i,j}} s_{i,j}(\alpha^{p^uq^vy^{k+l}}) + \sum_{i=0}^{m}\delta_{i,n+1}s_{i,n+1}(\alpha^{p^uq^v}) + \sum_{j=0}^{n}\delta_{m+1,j}s_{m+1,j}(\alpha^{p^uq^v}) + \delta_{m+1,n+1}.$$

If $0 \le u \le m$ and $0 \le v \le n$, then by Lemma 2.4

$$s(\alpha^t) = \sum_{l\in I_{m-u,n-v}} s_{m,n}(\alpha^{y^{k+l}}) + \sigma_{m-u,n-v} = \sum_{l\in I_{m-u,n-v}} T(\beta^{y^{k+l}}) + \sigma_{m-u,n-v}. \quad (2.8)$$

We conclude that $s(\alpha^t) = 0$ if and only if $\sum_{l\in I_{m-u,n-v}} T(\beta^{y^{k+l}}) \equiv \sigma_{m-u,n-v} \pmod 2$. Hence, the order of set $\{t \in \cup_{k=0}^{e-1}p^uq^vD_k|s(\alpha^t) = 0\}$ is $A_{m-u,n-v}p^{m-u}q^{n-v}R$, so the order of set $\{t \in \cup_{u=0}^{m}\cup_{v=0}^{n} p^uq^vZ_N^*|s(\alpha^t) = 0\}$ is $\sum_{u=0}^{m}\sum_{v=0}^{n}A_{u,v}p^uq^vR$.

If $u = m+1$ and $v \le n$, then by (2.2) and Lemma 2.4

$$s(\alpha^t) = \frac{p-1}{e}\sum_{i=0}^{m}|I_{i,n-v}| + \delta_{m+1,n-v} + \delta_{m+1,n+1} = \sigma_{m+1,n-v}. \quad (2.9)$$

We conclude that $s(\alpha^t) = 0$ if and only if $\sigma_{m+1,n-v} \equiv 0 \pmod 2$. Hence, the order of set $\{t \in p^{m+1}q^vZ_N^*|s(\alpha^t) = 0\}$ is $A_{m+1,n-v}q^{n-v}(q-1)$, so the order of set $\{t \in \cup_{v=0}^{n}p^{m+1}q^vZ_N^*|s(\alpha^t) = 0\}$ is $\sum_{v=0}^{n}A_{m+1,v}q^v(q-1)$.

If $u \le m$ and $v = n+1$, then by (2.2) and Lemma 2.4

$$s(\alpha^t) = \frac{q-1}{e}\sum_{j=0}^{m}|I_{m-u,j}| + \delta_{m-u,n+1} + \delta_{m+1,n+1} = \sigma_{m-u,n+1}. \quad (2.10)$$

Similarly, the order of set $\{t \in \cup_{u=0}^{m}p^uq^{n+1}Z_N^*|s(\alpha^t) = 0\}$ is $\sum_{u=0}^{m}A_{u,n+1}p^u(p-1)$.

If $u = m+1$ and $v = n+1$, then we conclude that $s(\alpha^0) = s(1) = 0$ if and only if $\delta_{m+1,n+1} = 0$ if and only if $I_{m+1,n+1} = \emptyset$.

TABLE I

even

	0	*1*	*2*	*3*
0	A	B	C	D
1	E	E	D	B
2	A	E	A	E
3	E	D	B	E

TABLE II

odd

	0	*1*	*2*	*3*
0	A	B	C	D
1	B	D	E	E
2	C	E	C	E
3	D	E	E	B

Hence by the definition of $E_{u,v}, F_{u,v}, A_{u,v}, \delta$, we get the linear complexity of the sequence defined as (1.5). □

III. Generalized Cyclotomic Sets of Order 4

In this section, we will assume that $\gcd(p-1, q-1) = e = 4$ and g is a primitive root of p and q. We will generalize the results from [8] and give values of Gauss periods of Whiteman's generalized cyclotomy of order 4 over $GF(2)$. Moreover, we determine b up to sign in Whiteman's generalized cyclotomic numbers of order 4 if $p \equiv q \equiv 5 \pmod 8$.

Since $\gcd(p-1, q-1) = 4$

$$\begin{aligned}\mathrm{ord}_{pq}(g) &= \mathrm{lcm}(\mathrm{ord}_p(g), \mathrm{ord}_q(g)) = \mathrm{lcm}(p-1, q-1)\\ &= \frac{(p-1)(q-1)}{4} = R.\end{aligned}$$

Whiteman [15] defined generalized cyclotomic classes

$$H_i = \{g^s y^i : s = 0, 1, \ldots, R-1\}, i = 0, 1, 2, 3, \quad (3.1)$$
$$y \equiv g \pmod p, y \equiv 1 \pmod q.$$

And we have $Z_{pq}^* = H_0 \cup H_1 \cup H_2 \cup H_3$.

The corresponding generalized cyclotomic numbers of order 4 are defined by

$$(i, j) = |(H_i + 1) \cap H_j|, \text{ for all } i, j = 0, 1, 2, 3.$$

By Gauss's theorem, there are exactly two representations over $\mathbb{Z}$

$$pq = a^2 + 4b^2,\ pq = a'^2 + 4b'^2,\ a \equiv a' \equiv 1 \pmod 4). \quad (3.2)$$

Lemma 3.1: The 16 cyclotomic numbers $(i, j), i, j = 0, 1, 2, 3$, depend solely upon one of the two decompositions in (3.2).

If $(p-1)(q-1)/16$ is even, then in Table I $8A = -a + 2M + 3$, $8B = -a - 4b + 2M - 1$, $8C = 3a + 2M - 1$, $8D = -a + 4b + 2M - 1$, $8E = a + 2M + 1$, where a, b is defined as (3.2) and $M = \frac{(p-2)(q-2)-1}{4}$.

If $(p-1)(q-1)/16$ is odd, then in Table II $8A = 3a+2M+5$, $8B = -a + 4b + 2M + 1$, $8C = -a + 2M + 1$, $8D = -a - 4b + 2M + 1$, $8E = a + 2M - 1$.

In fact, $\frac{(p-1)(q-1)}{16}$ is even if and only if $p \equiv q + 4 \pmod 8$; $\frac{(p-1)(q-1)}{16}$ is odd if and only if $p \equiv q \equiv 5 \pmod 8$.

Lemma 3.2: Let m_1, m_2 be two positive integers. The system of congruences

$$y \equiv t_1 \pmod{m_1}, \quad y \equiv t_2 \pmod{m_2}$$

has solutions if and only if

$$\gcd(m_1, m_2) | t_1 - t_2.$$

Proof: See [13, Theorem 2.9]. □

Lemma 3.3:

1) $-1 \in H_0$ if and only if $p \equiv q \equiv 5 \pmod 8$; $-1 \in H_2$ if and only if $p \equiv q + 4 \pmod 8$.
2) $2 \in H_0 \cup H_2$ if and only if $p \equiv q \equiv 5 \pmod 8$, and $2 \in H_1 \cup H_3$ if and only if $p \equiv q + 4 \pmod 8$.
3) Let $p \equiv q \equiv 5 \pmod 8$ and
$$2 \equiv g^{t_1} \pmod p,\ 2 \equiv g^{t_2} \pmod q. \quad (3.3)$$
Then $2 \in H_0$ if and only only if $4 | t_1 - t_2$; in other words, $2 \in H_2$ if and only if $4 \nmid t_1 - t_2$.

Proof:

1) Since g is a primitive root of p and q, $-1 \equiv g^{t_1} \pmod p$ and $-1 \equiv g^{t_2} \pmod q$.
If $p \equiv q \equiv 5 \pmod 8$, then $2 \| t_1$ and $2 \| t_2$ (see [10]), so $4 | t_1 - t_2$. Hence, there is $k \in Z$ such that $k \equiv t_1 \pmod{p-1}$ and $k \equiv t_2 \pmod{q-1}$, so by Lemma 3.2 $-1 \equiv g^k \pmod{pq}$ and $-1 \in H_0$. If $p \equiv 1 \pmod 8$ and $q \equiv 5 \pmod 8$, then $4 | t_1$ and $2 \| t_2$, so $4 | t_1 - t_2 - 2$. Hence, there exists $k \in Z$ such that $k \equiv t_1 - 2 \pmod{p-1}$ and $k \equiv t_2 \pmod{q-1}$. Thus by Lemma 3.2 $-1 \equiv y^2 g^k \pmod{pq}$ and $-1 \in H_2$, where y is defined as (3.1). The converse is straightforward.
2) Let $2 \equiv g^{t_1} \pmod p$ and $2 \equiv g^{t_2} \pmod q$. If $p \equiv q \equiv 5 \pmod 8$, then $2 \nmid t_1$ and $2 \nmid t_2$, so $2 | t_1 - t_2$. Similarly, we have $2 \in H_0 \cup H_2$. If $p \equiv 1 \pmod 8$ and $q \equiv 5 \pmod 8$, then $2 | t_1$ and $2 \nmid t_2$, so $2 \nmid t_1 - t_2$. Similarly, we have $2 \in H_1 \cup H_3$. The converse is straightforward.
3) Since $p \equiv q \equiv 5 \pmod 8$, t_1 and t_2 are odd in (3.3), so $2 | t_1 - t_2$. By Lemma 3.2, we conclude that $4 | t_1 - t_2$ if and only if there is $k \in Z$ such that $k \equiv t_1 \pmod{p-1}$ and $k \equiv t_2 \pmod{q-1}$ if and only if $2 \equiv g^k \pmod{pq}$ and $2 \in H_0$. Moreover, we have that $4 \nmid t_1 - t_2$ if and only if $4 | t_1 - t_2 - 2$ if and only if there is $k \in \mathbb{Z}$ such that $k \equiv t_1 - 2 \pmod{p-1}$ and $k \equiv t_2 \pmod{q-1}$ if and only if $2 \equiv y^2 g^k \pmod{pq}$ and $2 \in H_2$, where y is defined as (3.1). □

We define
$P = \{p, 2p, \ldots, (q-1)p\}, Q = \{q, 2q, \cdots, (p-1)q\}$.

Lemma 3.4: For each $\omega \in P \cup Q$

$$|H_i \cap (H_j + \omega)| = \begin{cases} \frac{(p-1)(q-1)}{16}, & \text{if } i \neq j \\ \frac{(p-1)(q-5)}{16}, & \text{if } i = j, p|\omega \\ \frac{(p-5)(q-1)}{16}, & \text{if } i = j, q|\omega. \end{cases}$$

Proof: See [15, Lemmas 2 and 4]. □

Lemma 3.5: Let $p \equiv q \equiv 5 \pmod 8$. Then there are exactly two representations over $\mathbb{Z}$

$$pq = a^2 + 4b^2 = a'^2 + 4b'^2,\ a \equiv a' \equiv 1 \pmod 4 \tag{3.4}$$

where one of b and b' is divided by 4 and another is exactly divided by 2.

Proof: Let $p = x_1^2 + 4y_1^2$ and $q = x_2^2 + 4y_2^2$, $x_j, y_j \in Z, j = 1, 2$; then $2 \nmid y_j, j = 1, 2$ by $p \equiv q \equiv 5 \pmod 8$. Hence, $pq = a^2 + 4b^2 = a'^2 + 4b'^2$, $b = x_1y_2 + x_2y_1$, and $b' = x_1y_2 - x_2y_1$, where one of b and b' is divided by 4 and another is exactly divided by 2. □

Let $T(x) = \sum_{l \in H_0} x^l$ and β a pqth primitive root of unity in the extension over $GF(2)$. Define

$$T_4(\beta) = (T(\beta), T(\beta^y), T(\beta^{y^2}), T(\beta^{y^3})) \tag{3.5}$$

where y is defined as (3.1) or (1.1).

Lemma 3.6: If $p \equiv q + 4 \pmod 8$, then $T_4(\beta) = (\gamma, \gamma^2, \gamma^4, \gamma^8)$ or $T_4(\beta) = (\gamma, \gamma^8, \gamma^4, \gamma^2)$, where $\gamma^4 + \gamma^3 + \gamma^2 + \gamma + 1 = 0$ or $\gamma^4 + \gamma^3 + 1 = 0$.

Proof: If $p \equiv q + 4 \pmod 8$, then by Lemma 3.3 $2 \in H_1 \cup H_3$. Suppose that $2 \in H_1$; then $T(\beta)^2 = \sum_{l \in H_0} \beta^{2l} = \sum_{l \in H_1} \beta^l = T(\beta^y)$. Similarly, $T(\beta)^4 = T(\beta^{y^2})$, $T(\beta)^8 = T(\beta^{y^3})$. Set $\gamma := T(\beta)$; then $T_4(\beta) = (\gamma, \gamma^2, \gamma^4, \gamma^8)$ satisfies $\gamma + \gamma^2 + \gamma^4 + \gamma^8 = 1$, so $\gamma^4 + \gamma^3 + \gamma^2 + \gamma + 1 = 0$ or $\gamma^4 + \gamma^3 + 1 = 0$. Suppose that $2 \in H_3$; then $T_4(\beta) = (\gamma, \gamma^8, \gamma^4, \gamma^2)$. □

The following is a well-known result.

Lemma 3.7: Let $p \equiv q \equiv 5 \pmod 8$ be distinct primes with $\gcd(p-1, q-1) = 4$. Fix g a common primitive root of p and q. Then $2 \in H_0$ if and only if $T(\beta^{y^i}) \in GF(2), i = 0, 1, 2, 3$; $2 \in H_2$ if and only if either $T(\beta), T(\beta^{y^2}) \in GF(2)$ or $T(\beta^y), T(\beta^{y^3}) \in GF(2)$.

Now we give the values of $T_4(\beta)$ clearly.

Theorem 3.8: Let β be a pqth primitive root of unity. Suppose that the cyclotomic numbers of Lemma 3.1 depend upon the decomposition $pq = a^2 + 4b^2, a \equiv 1 \pmod 4$. Let $T_4(\beta) = (T(\beta), T(\beta^y), T(\beta^{y^2}), T(\beta^{y^3}))$. Then by a choice of β (i.e., a pqth primitive root of unity), we have:

1) $T_4(\beta) = (0,0,1,0)$ or $(1,0,0,0)$, if $a \equiv 1 \pmod 8$ and $4|b$;
2) $T_4(\beta) = (0,1,1,1)$ or $(1,1,0,1)$, if $a \equiv 5 \pmod 8$ and $4|b$;
3) $T_4(\beta) = (\mu, 1, \mu+1, 1)$ or $(\mu+1, 1, \mu, 1)$, if $a \equiv 1 \pmod 8$ and $2\|b$;
4) $T_4(\beta) = (\mu, 0, \mu+1, 0)$ or $(\mu+1, 0, \mu, 0)$, if $a \equiv 5 \pmod 8$ and $2\|b$;
5) $T_4(\beta) = (\gamma, \gamma^2, \gamma^4, \gamma^8)$ or $(\gamma, \gamma^8, \gamma^4, \gamma^2)$, if $b \equiv 1 \pmod 2$;

where μ satisfies $\mu^2 + \mu + 1 = 0$, and γ satisfies either $\gamma^4 + \gamma^3 + \gamma^2 + \gamma + 1 = 0$ or $\gamma^4 + \gamma^3 + 1 = 0$.

Proof: Set

$$\Psi_i := T(\beta^{y^i}), i = 0, 1, 2, 3.$$

If $p \equiv q \equiv 5 \pmod 8$, then $-1 \in H_0$, and then by Lemmas 3.1, 3.3, and 3.4

$$\begin{aligned}
\Psi_0\Psi_2 &= \sum_{l \in H_0} \beta^l \sum_{m \in H_2} \beta^m = \sum_{l \in H_0} \sum_{m \in H_2} \beta^{l-m} \\
&= (2,0)\Psi_0 + (1,3)\Psi_1 + (0,2)\Psi_2 + (3,1)\Psi_3 \\
&\quad - \frac{(p-1)(q-1)}{8} \\
&= C(\Psi_0 + \Psi_2) + E(\Psi_1 + \Psi_3) - \frac{(p-1)(q-1)}{8} \\
&= \frac{-a+1}{4}(\Psi_0 + \Psi_2) + \frac{a + 2M - 1}{8} - \frac{(p-1)(q-1)}{8} \\
&= \frac{-a+1}{4}(\Psi_0 + \Psi_2) + \frac{-4b^2 - a^2 + 2a - 1}{16} \\
\Psi_1\Psi_3 &= \sum_{l \in H_1} \beta^l \sum_{m \in H_3} \beta^m = \sum_{l \in H_1} \sum_{m \in H_3} \beta^{l-m} \\
&= (3,1)\Psi_0 + (2,0)\Psi_1 + (1,3)\Psi_2 + (0,2)\Psi_3 \\
&\quad - \frac{(p-1)(q-1)}{8} \\
&= E(\Psi_0 + \Psi_2) + C(\Psi_1 + \Psi_3) - \frac{(p-1)(q-1)}{8} \\
&= \frac{-a+1}{4}(\Psi_1 + \Psi_3) + \frac{-4b^2 - a^2 + 2a - 1}{16}.
\end{aligned}$$

If $p \equiv q \equiv 5 \pmod 8$, then by Lemma 3.5 set $a = 4s + 1$, $b = 2t$, $s, t \in Z$, and then we have

$$\Psi_0\Psi_2 = s(\Psi_0 + \Psi_2) - t^2 - s^2 \tag{3.6}$$

$$\Psi_1\Psi_3 = s(\Psi_1 + \Psi_3) - t^2 - s^2. \tag{3.7}$$

By Lemma 3.3, we have $2 \in H_0 \cup H_2$ and by Lemma 3.7 we have $\Psi_0 + \Psi_2,\ \Psi_1 + \Psi_3 \in GF(2)$. Since $\Psi_0 + \Psi_1 + \Psi_2 + \Psi_3 = 1$, without loss of generality (i.e., by a choice of β) we may assume that

$$\Psi_0 + \Psi_2 = 1, \Psi_1 + \Psi_3 = 0. \tag{3.8}$$

Then by (3.6) and (3.7), we have

$$\Psi_0\Psi_2 = s - t^2 - s^2 \equiv t \pmod 2,\ \Psi_1\Psi_3 = -t^2 - s^2 \equiv s + t \pmod 2. \tag{3.9}$$

Solving systems (3.8) and (3.9), we obtain:

1) $T_4(\beta) = (0,0,1,0)$ or $(1,0,0,0)$, if $s \equiv 0 \pmod 2$ and $t \equiv 0 \pmod 2$;
2) $T_4(\beta) = (0,1,1,1)$ or $(1,1,0,1)$, if $s \equiv 1 \pmod 2$ and $t \equiv 0 \pmod 2$;
3) $T_4(\beta) = (\mu, 1, \mu+1, 1)$ or $(\mu+1, 1, \mu, 1)$, if $s \equiv 0 \pmod 2$ and $t \equiv 1 \pmod 2$;
4) $T_4(\beta) = (\mu, 0, \mu+1, 0)$ or $(\mu+1, 0, \mu, 0)$, if $s \equiv 1 \pmod 2$ and $t \equiv 1 \pmod 2$;

where μ is a root of the equation $x^2 + x + 1 = 0$.

If $p \equiv q + 5 \pmod 8$, then b is odd and (5) is clear from Lemma 3.6. □

Corollary 3.9: Let $p \equiv q \equiv 5 \pmod 8$. Fix a common primitive root g of p and q. Then $2 \in H_0$ if and only if the generalized cyclotomic numbers of Lemma 3.1 depend on the decomposition $N = a^2 + 4b^2$ with $4|b$; $2 \in H_2$ if and only if the generalized cyclotomic numbers depend on the decomposition $N = a^2 + 4b^2$ with $2\|b$.

Proof: It is clear from Lemma 3.7 and Theorem 3.8 □

By Corollary 3.9 and Lemma 3.3, we can determine b up to sign in Whiteman's generalized cyclotomic numbers of order 4 in the case $p \equiv q \equiv 5 \pmod 8$ if fixing a common primitive root g of p and q.

IV. Applications

A. Sequence of Period pq

We can use the method in Sections II and III to compute the linear complexity of the generalized cyclotomic pq-periodic binary sequence of order 4 in [1]. But we can not use the method in [1] to calculate the linear complexity of the following sequence.

The generalized cyclotomic pq-periodic binary sequence s of order 4 with respect to the primes p and q is defined as

$$s_i = \begin{cases} 1, & \text{if } i \pmod N \in \Omega \\ 0, & \text{otherwise} \end{cases} \tag{4.1}$$

where $P = \{p, 2p, \ldots, (q-1)p\}$ and $\Omega = P \cup H_0$.

Now we compute the linear complexity L and the minimal polynomial $m(x)$ of Whiteman's generalized cyclotomic sequence of order 4. Let β be a pqth primitive root of unity in an extension over $GF(2)$. Set

$$d_i(x) = \prod_{l \in H_i} (x - \beta^l), i = 0, 1, 2, 3.$$

By Theorem 2.5 and 3.8, we can get the following result.

Theorem 4.1:

(I) If $p \equiv 1 \pmod 8$ and $q \equiv 5 \pmod 8$, then

$$L = pq - 1, \quad m(x) = \frac{x^{pq} - 1}{x - 1}.$$

(II) If $p \equiv 5 \pmod 8$ and $q \equiv 1 \pmod 8$, then

$$L = pq - p - q + 1, \quad m(x) = \frac{(x^{pq} - 1)(x - 1)}{(x^p - 1)(x^q - 1)}.$$

(III) Let $2 \in H_0$ and $pq \equiv 1 \pmod{16}$. Then

$$L = \frac{(p-1)(3q+1)}{4}, \quad m(x) = \frac{x^{pq} - 1}{d_0(x)(x^q - 1)}.$$

(IV) Let $2 \in H_0$ and $pq \equiv 9 \pmod{16}$. Then

$$L = \frac{(p-1)(q+3)}{4}, \quad m(x) = \frac{(x^p - 1)d_0(x)}{x - 1}.$$

(V) Let $2 \in H_2$ and $pq \equiv 1 \pmod{16}$. Then

$$L = \frac{(p-1)(q+1)}{2}, \quad m(x) = \frac{x^{pq} - 1}{d_1(x)d_3(x)(x^q - 1)}.$$

(VI) Let $2 \in H_2$ and $pq \equiv 9 \pmod{16}$. Then

$$L = pq - q, \quad m(x) = \frac{x^{pq} - 1}{x^q - 1}.$$

Proof: By Theorems 2.5 and 3.8, we compute the linear complexity of the sequence s defined as (4.1). About Theorem 2.5, we know that $n = m = 0$, $D_0^{(0,0)} = H_0$, $D_0^{(1,0)} = pZ_{pq}^* = P$, $\delta_{1,0} = 1$, $\delta_{0,1} = 0$, $\delta_{1,1} = 0$, $\sigma_{0,0} = 1$, $\sigma_{1,0} \equiv \frac{p-1}{4} + 1 \pmod 2$, $\sigma_{0,1} \equiv \frac{q-1}{4} \pmod 2$, $\delta = 1$.

(I) If $p \equiv 1 \pmod 8$ and $q \equiv 5 \pmod 8$, then $\sigma_{1,0} \equiv 1 \pmod 2$, $\sigma_{0,1} \equiv 1 \pmod 2$, and $E_{0,0} = F_{0,0} = 0$ by Theorem 3.8. Hence, $A_{0,0} = A_{1,0} = A_{0,1} = 0$, so by Theorem 2.5

$$L = pq - 1, m(x) = \frac{x^{pq} - 1}{x - 1}.$$

(II) If $p \equiv 5 \pmod 8$ and $q \equiv 1 \pmod 8$, then $\sigma_{1,0} \equiv 0 \pmod 2$, $\sigma_{0,1} \equiv 0 \pmod 2$, and $E_{0,0} = F_{0,0} = 0$. Hence, $A_{0,0} = 0$, $A_{1,0} = A_{0,1} = 1$, so

$$L = pq - (p-1) - (q-1) - 1 = pq - p - q + 1$$

$$m(x) = \frac{(x^{pq} - 1)(x - 1)}{(x^p - 1)(x^q - 1)}.$$

(III) If $2 \in H_0$ and $pq \equiv 1 \pmod{16}$, then $\sigma_{1,0} \equiv 0 \pmod 2$, $\sigma_{0,1} \equiv 1 \pmod 2$, $E_{0,0} = 3$, and $F_{0,0} = 1$. Hence, $A_{0,0} = 1$, $A_{1,0} = 1$, and $A_{0,1} = 0$, so

$$L = pq - \frac{(p-1)(q-1)}{4} - (q-1) - 1 = \frac{(p-1)(3q+1)}{4}.$$

Choosing β with $T_4(\beta) = (1, 0, 0, 0)$ in Theorem 3.8 (1), we have

$$m(x) = \frac{x^{pq} - 1}{d_0(x)(x^q - 1)}.$$

(IV) If $2 \in H_0$ and $pq \equiv 9 \pmod{16}$, then $\sigma_{1,0} \equiv 0 \pmod 2$, $\sigma_{0,1} \equiv 1 \pmod 2$, $F_{0,0} = 3$. Hence, $A_{0,0} = 3$, $A_{1,0} = 1$, and $A_{0,1} = 0$, so

$$L = pq - 3\frac{(p-1)(q-1)}{4} - (q-1) - 1 = \frac{(p-1)(q+3)}{4}.$$

Choosing β with $T_4(\beta) = (0, 1, 1, 1)$ in Theorem 3.8 (2), we have

$$m(x) = \frac{x^{pq} - 1}{d_1(x)d_2(x)d_3(x)(x^q - 1)} = \frac{(x^p - 1)d_0(x)}{x - 1}.$$

(V) If $2 \in H_2$ and $pq \equiv 1 \pmod{16}$, then $\sigma_{1,0} \equiv 0 \pmod 2$, $\sigma_{0,1} \equiv 1 \pmod 2$, $F_{0,0} = 2$. Hence, $A_{0,0} = 2$, $A_{1,0} = 1$, and $A_{0,1} = 0$, so

$$L = pq - 2\frac{(p-1)(q-1)}{4} - (q-1) - 1 = \frac{(p-1)(q+1)}{2}.$$

Choosing β with $T_4(\beta) = (\mu, 1, \mu + 1, 1)$ in Theorem 3.8 (3), we have

$$m(x) = \frac{x^{pq} - 1}{d_1(x)d_3(x)(x^q - 1)}.$$

(VI) If $2 \in H_2$ and $pq \equiv 9 \pmod{16}$, then $\sigma_{1,0} \equiv 0 \pmod 2$, $\sigma_{0,1} \equiv 1 \pmod 2$, $F_{0,0} = 0$. Hence, $A_{0,0} = 0$, $A_{1,0} = 1$, $A_{0,1} = 0$, so

$$L = pq - (q-1) - 1 = pq - q, \ m(x) = \frac{x^{pq} - 1}{x^q - 1}.$$

□

B. Sequence of Period $N = p^{m+1}q^{n+1}$

Suppose $\Omega = \bigcup_{i=0}^{m}\bigcup_{j=0}^{n} p^i q^j D_0^{(i,j)}$ $(m > 0,\ n > 0)$ and

$$s_i = \begin{cases} 1, & \text{if } i \pmod N \in \Omega \\ 0, & \text{otherwise.} \end{cases} \tag{4.2}$$

Then by Theorem 2.5, we get the linear complexity of the sequence in (4.2).

Theorem 4.2: Let m_2 and n_2 be the largest even integers such that $m_2 \le m$ and $n_2 \le n$, respectively. Let m_1 and n_1 be the largest odd integers such that $m_1 \le m$ and $n_1 \le n$, respectively.

(1) Suppose that $p \equiv 1 \pmod 8, q \equiv 5 \pmod 8$; then

$$L = (p^{m+1} - 1)(q^{n+1} - \delta_n)$$

where

$$\delta_n = \begin{cases} 0, & \text{if n is even} \\ 1, & \text{if } n \text{ is odd.} \end{cases}$$

(2) Suppose that $p \equiv q \equiv 5 \pmod 8$.

(I) If $2 \in H_0$ and $pq \equiv 1 \pmod{16}$, then see the first equation shown at the bottom of the page.

(II) If $2 \in H_0$ and $pq \equiv 9 \pmod{16}$, then see the second equation shown at the bottom of the page.

(III) If $2 \in H_2$ and $pq \equiv 1 \pmod{16}$, then see the third equation shown at the bottom of the page.

(IV) If $2 \in H_2$ and $pq \equiv 9 \pmod{16}$, then see the fourth equation shown at the bottom of the page.

Proof: By Theorems 2.5 and 3.8, we compute the linear complexity of the sequence. About Theorem 2.5, we know that $\delta_{i,n+1} = 0, i = 0, 1, \ldots, m, \delta_{m+1,j} = 0,\ j = 0, 1, \ldots, n+1$, $\sigma_{u,v} = \frac{q-1}{4}(n-v) + \frac{p-1}{4}(m-u)$, $\sigma_{u,n+1} = \frac{q-1}{4}(n+1)$, $\sigma_{m+1,v} = \frac{p-1}{4}(m+1)$ for $0 \le u \le m, 0 \le v \le n$, and $\delta = 1$.

1) Since $p \equiv 1 \pmod 8$ and $q \equiv 5 \pmod 8$, by Lemma 3.6 we know $E_{u,v} = 0 = F_{u,v}$, so $A_{u,v} = 0$ for $0 \le u \le m$ and $0 \le v \le n$. By $\sigma_{m+1,v} = \frac{p-1}{4}\sum_{i=0}^{m}|I_{i,v}| \equiv 0 \pmod 2$, $\sigma_{u,n+1} = \frac{q-1}{4}\sum_{j=0}^{n}|I_{u,j}| \equiv n+1 \pmod 2$. Hence, by Theorem 2.5 we have

$$\begin{aligned} L &= N - \sum_{v=0}^{n} q^v(q-1) - \delta_n \sum_{u=0}^{m} p^u(p-1) - 1 \\ &= (p^{m+1} - 1)(q^{n+1} - \delta_n) \end{aligned}$$

where $\delta_n = 1$ if n is odd and $\delta_n = 0$ if n is even.

2) If $p \equiv q \equiv 5 \pmod 8$

(I) If $2 \in H_0$ and $pq \equiv 1 \pmod{16}$, then for $0 \le u \le m$ and $0 \le v \le n$, by Theorem 3.8 $E_{u,v} = 3$ and $F_{u,v} = 1$, $\sigma_{u,v} = \frac{p-1}{4}\sum_{j=v+1}^{n}|I_{u,j}| + \frac{q-1}{4}\sum_{i=u+1}^{m}|I_{i,v}| \equiv m - u + n - v \pmod 2$, $\sigma_{u,n+1} \equiv n+1 \pmod 2$, and $\sigma_{m+1,v} \equiv m+1 \pmod 2$. Hence, we have

$$L = N - \sum_{u=0}^{m}\sum_{v=0}^{n} p^u q^v R - 2\sum_{m+n-u-v \text{ even}} p^u q^v R - \delta_m(q^{n+1} - 1) - \delta_n(p^{m+1} - 1) - 1.$$

$$L = N - \frac{(p^{m+1} - 1)(q^{n+1} - 1)}{4} - \delta_m(q^{n+1} - 1) - \delta_n(p^{m+1} - 1) - 1 - \frac{(p^{m+2} - p^{m-m_2})(q^{n+2} - q^{n-n_2}) + (p^{m+1} - p^{m-m_1})(q^{n+1} - q^{n-n_1})}{2(p+1)(q+1)}$$

$$L = N - \frac{(p^{m+1} - 1)(q^{n+1} - 1)}{4} - \delta_m(q^{n+1} - 1) - \delta_n(p^{m+1} - 1) - 1 - \frac{(p^{m+2} - p^{m-m_2})(q^{n+1} - q^{n-n_1}) + (p^{m+1} - p^{m-m_1})(q^{n+2} - q^{n-n_2})}{2(p+1)(q+1)}$$

$$L = N - \delta_m(q^{n+1} - 1) - \delta_n(p^{m+1} - 1) - 1 - \frac{(p^{m+2} - p^{m-m_2})(q^{n+1} - q^{n-n_1}) + (p^{m+1} - p^{m-m_1})(q^{n+2} - q^{n-n_2})}{2(p+1)(q+1)}$$

$$L = N - \delta_m(q^{n+1} - 1) - \delta_n(p^{m+1} - 1) - 1 - \frac{(p^{m+2} - p^{m-m_2})(q^{n+2} - q^{n-n_2}) + (p^{m+1} - p^{m-m_1})(q^{n+1} - q^{n-n_1})}{2(p+1)(q+1)}$$

Moreover, we have the first equation shown at the bottom of the page. Hence, we prove (I).

(II) If $2 \in H_0$ and $pq \equiv 9 \pmod{16}$, then $E_{u,v} = 1$ and $F_{u,v} = 3$ for $0 \le u \le m$ and $0 \le v \le n$. Similarly, we have

$$L = N - \sum_{u=0}^{m}\sum_{v=0}^{n} p^u q^v R - 2\sum_{m+n-u-v \text{ odd}} p^u q^v R - \delta_m(q^{n+1}-1) - \delta_n(p^{m+1}-1) - 1.$$

Moreover, we have the second equation shown at the bottom of the page. Hence, we prove (II).

(III) If $2 \in H_2$ and $pq \equiv 1 \pmod{16}$, then by Theorem 3.8 $E_{u,v} = 0$ and $F_{u,v} = 2$ for $0 \le u \le m$ and $0 \le v \le n$. Similarly, we have

$$L = N - 2\sum_{m+n-u-v \text{ odd}} p^u q^v R - \delta_m(q^{n+1}-1) - \delta_n(p^{m+1}-1) - 1.$$

So we prove (III).

(IV) If $2 \in H_0$ and $pq \equiv 9 \pmod{16}$, then by Theorem 3.8 $E_{u,v} = 2$ and $F_{u,v} = 0$ for $0 \le u \le m$ and $0 \le v \le n$. Similarly, we have

$$L = N - 2\sum_{m+n-u-v \text{ even}} p^u q^v R - \delta_m(q^{n+1}-1) - \delta_n(p^{m+1}-1) - 1.$$

So we prove (IV). □

V. Open Problem

If $p \equiv q + 4 \pmod 8$, how do Whiteman's generalized cyclotomic numbers of order 4 depend on the two decompositions $pq = a^2 + 4b^2 = a'^2 + 4b'^2, a \equiv a' \equiv 1 \pmod 4$?

Acknowledgment

The authors are grateful to the two anonymous referees for their valuable comments and suggestions that much improved this paper.

References

[1] E. Bai, X. Fu, and G. Xiao, "On the linear complexity of generalized cyclotomic sequences of order four over Z_{pq}," *IEICE Trans. Fundam.*, vol. 88-A (I), pp. 392–395, 2005.

[2] E. Bai and X. Liu, "Some notes on prime-square sequences," *J. Comput. Sci. Technol.*, vol. 22, no. 3, pp. 481–486, 2007.

[3] C. Ding, "Linear complexity of generalized cyclotomic binary sequences of order 2," *Finite Fields Appl.*, vol. 3, pp. 159–174, 1997.

[4] C. Ding, "Autocorrelation values of generalized cyclotomic sequences of order two," *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp. 1698–1702, Jul. 1998.

[5] C. Ding and T. Helleseth, "New generalized cyclotomy and its application," *Finite Fields Appl.*, vol. 4, pp. 140–166, 1998.

[6] C. Ding and T. Helleseth, "Generalized cyclotomic codes of length $p_1^{e_1}\cdots p_t^{e_t}$," *IEEE Trans. Inf. Theory*, vol. 45, no. 2, pp. 467–474, Mar. 1999.

[7] C. Ding, T. Helleseth, and K. Y. Lam, "Several classes of binary sequences with three-level autocorrelation," *IEEE Trans. Inform. Theory*, vol. 45, no. 7, pp. 2601–2606, Nov. 1999.

[8] V. A. Edemskii, "On the linear complexity of binary sequences on the basis of biquadratic and sextic residue classes," *Discret. Math. Appl.*, vol. 20, no. 1, pp. 75–84, 2010.

[9] V. A. Edemskiy, "About computation of the linear complexity of generalized cyclotomic sequences with period p^{n+1}," *Des. Codes Cryptogr.*, vol. 61, no. 3, pp. 251–260, 2011.

[10] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory, GTM 84*. Berlin, Germany: Springer-Verlag, 1982.

[11] R. Lidl and H. Neiderreiter, *Finite Fields*. Reading, MA: Addison-Wesley, 1983.

[12] F. Liu, D. Peng, Z. Zhou, and X. Tang, "A new frequency-hopping sequence set based upon generalized cyclotomy," *Designs, Codes, Cryptogr.*, 2012, DOI: 10.1007/s10623-012-9652-z.

[13] M. B. Nathanson, *Elementary Methods in Number Theory, GTM195*. Berlin, Germany: Springer-Werlag, 2000.

[14] T. Yan, R. Sun, and G. Xiao, "Autocorraltion and linear complexity of the new generalized cyclotomic sequences," *IEICE Trans. Fundam. Electron.*, vol. E90-A, pp. 857–864, 2007.

[15] A. L. Whiteman, "A family of difference sets," *Illinois J. Math.*, vol. 6, pp. 107–121, 1962.

$$\sum_{u=0}^{m}\sum_{v=0}^{n} p^u q^v R = R\sum_{u=0}^{m} p^u \sum_{v=0}^{n} q^v = \frac{(p^{m+1}-1)(q^{n+1}-1)}{4},$$

$$\begin{aligned}\sum_{m-u+n-v \text{ even}} p^u q^v R &= \sum_{u+v \text{ even}} p^{m-u} q^{n-v} R = p^m q^n R \sum_{u+v \text{ even}} p^{-u} q^{-v}\\ &= p^m q^n R[(1+p^{-2}+\cdots+p^{-m_2})(1+q^{-2}+\cdots+q^{-n_2})\\ &\quad +(p^{-1}+p^{-3}\cdots+p^{-m_1})(q^{-1}+q^{-3}+\cdots+q^{-n_1})]\\ &= \frac{(p^{m+2}-p^{m-m_2})(q^{n+2}-q^{n-n_2})+(p^{m+1}-p^{m-m_1})(q^{n+1}-q^{n-n_1})}{4(p+1)(q+1)}\end{aligned}$$

$$\begin{aligned}\sum_{m-u+n-v \text{ odd}} p^u q^v R &= \sum_{u+v \text{ odd}} p^{m-u} q^{n-v} R = p^m q^n R \sum_{u+v \text{ odd}} p^{-u} q^{-v}\\ &= p^m q^n R[(1+p^{-2}+\cdots+p^{m_2})(q^{-1}+q^{-3}+\cdots+q^{-n_1})\\ &\quad +(p^{-1}+p^{-3}+\cdots+p^{-m_1})(1+q^{-2}+\cdots+q^{-n_2})]\\ &= \frac{(p^{m+2}-p^{m-m_2})(q^{n+1}-q^{n-n_1})+(p^{m+1}-p^{m-m_1})(q^{n+2}-q^{n-n_2})}{4(p+1)(q+1)}\end{aligned}$$

Liqin Hu received the M.S. degree in mathematics from the Nanjing University of Aeronautics and Astronautics, Nanjing, China. She is a Ph.D. student in Mathematics Department, Nanjing University of Aeronautics and Astronautics.

Qin Yue received the Ph.D. degree in mathematics from the University of Science and Technology of China, Hefei, China. He is a Professor in Mathematics Department, Nanjing University of Aeronautics and Astronautics. His research fields are algebraic number theory, cryptography, and coding theory.

Minhong Wang (M'10) received the Ph.D. degree in information systems from City University of Hong Kong in 2005. She is an Assistant Professor in the Faculty of Education, The University of Hong Kong.