Linear Complexity and Autocorrelation of Prime Cube Sequences

Young-Joon Kim, Seok-Yong Jin, and Hong-Yeop Song

Department of Electrical and Electronic Engineering
Yonsei University, Seoul, 121-749, Korea
{yj.kim, sy.jin, hysong}@yonsei.ac.kr

Abstract. We review a binary sequence based on the generalized cyclotomy of order 2 with respect to p^3, where p is an odd prime. Linear complexities, minimal polynomials and autocorrelation of these sequences are computed.

1 Introduction

Let $n \geq 2$ be a positive integer and Z_n^* be the multiplicative group of the integer ring Z_n. For a partition $\{D_i | i = 0, 1, \cdots, d-1\}$ of Z_n^*, if there exist elements $g_1, \cdots, g_d$ of Z_n^* satisfying $D_i = g_i D_0$ for all i where D_0 is a multiplicative subgroup of Z_n^*, the D_i are called *generalized cyclotomic classes* of order d. In 1998, Ding and Helleseth [1] introduced the new generalized cyclotomy with respect to $p_1^{e_1} \cdots p_t^{e_t}$ and defined a *balanced* binary sequence based on their own generalized cyclotomy, where $p_1, \cdots, p_t$ are distinct odd primes and $e_1, \cdots, e_t$ are positive integers. Before them, there have been lots of studies about cyclotomy, but they are only about ones with respect to p or p^2 or pq where p and q are distinct odd primes [1,4,7,8]. In [1] they also introduced how to construct a balanced binary sequence based on their generalized cyclotomy. Let it call the generalized cyclotomic sequences. Those sequences includes the binary quadratic residue sequences also known as Legendre Sequences because these sequences can be understood as the generalized cyclotomic sequences with respect to p.

In 1998, C. Ding [4] presented some cyclotomy sequences with period p^2 which are not balanced. They are defined in a slightly different way from the generalized cyclotomic sequences with respect to p^2. In that paper, he calculated the linear complexities with minor errors. Y.-H. Park and others [5] corrected the errors. The linear complexity of the sequence is not so good. In general, the linear complexity of a sequence is considered as good when it is not less than half of the period of the sequence. Recently, in [7], Yan *et al.* calculated the linear complexity and autocorrelation of generalized cyclotomic sequences of order 2 with respect to p^2.

In this paper, we compute the linear complexity and autocorrelation of the generalized cyclotomic sequences with respect to p^3. Hereafter we will call these sequences as *prime cube sequences*.

S. Boztaş and H.F. Lu (Eds.): AAECC 2007, LNCS 4851, pp. 188–197, 2007.
© Springer-Verlag Berlin Heidelberg 2007

2 Prime Cube Sequences

Let p be an odd prime. Let g be a primitive root of p^2. Then it's well known that g is also a primitive root of p^k for $k \geq 1$[2]. The order of g modulo p is $p-1$, the order of g modulo p^2 is $p(p-1)$ and the order of g modulo p^3 is $p^2(p-1)$.

Define

$$\begin{array}{llll} D_0^{(p)} = (g^2) & \pmod{p} & D_1^{(p)} = gD_0^{(p)} & \pmod{p} \\ D_0^{(p^2)} = (g^2) & \pmod{p^2} & D_1^{(p^2)} = gD_0^{(p^2)} & \pmod{p^2} \\ D_0^{(p^3)} = (g^2) & \pmod{p^3} & D_1^{(p^3)} = gD_0^{(p^3)} & \pmod{p^3} \end{array}$$

Then $Z_p^* = D_0^{(p)} \cup D_1^{(p)}, Z_{p^2}^* = D_0^{(p^2)} \cup D_1^{(p^2)}$ and $Z_{p^3}^* = D_0^{(p^3)} \cup D_1^{(p^3)}$. For $i = 0,1,2$, the $D_j^{(p^i)}$ are called generalized cyclotomic classes of order 2 with respect to p^j. Note that

$$Z_{p^3} = D_0^{(p^3)} \cup D_1^{(p^3)} \cup pD_0^{(p^2)} \cup pD_1^{(p^2)} \cup p^2 D_0^{(p)} \cup p^2 D_1^{(p)} \cup \{0\}.$$

Here and hereafter, $\frac{p^3}{p^i} D_j^{(p^i)}$ are sets of elements obtained by multiplying $\frac{p^3}{p^i}$ to the elements of $D_j^{(p^i)}$ over Z_{p^3} for $i = 0,1,2$ and $j = 0,1$.

In [1], the authors define the binary prime cube sequence $\{s(n)\}$ as follows[1]:

$$s(i) = \begin{cases} 0, & \text{if } (i \bmod p^3) \in C_0 \\ 1, & \text{if } (i \bmod p^3) \in C_1 \ . \end{cases} \tag{1}$$

where $C_0 = \bigcup_{d|p^3, d>1} \frac{p^3}{d} D_0^{(d)}$ and $C_1 = \{0\} \cup \bigcup_{d|p^3, d>1} \frac{p^3}{d} D_1^{(d)}$.

3 Linear Complexity and Minimal Polynomial

Let $\{s(n)\}$ be a sequence of period L over a field F. The linear complexity of $\{s(n)\}$ is defined to be least positive integer l such that there are constants $c_0 = 1, c_1, \cdots, c_l \in F$ satisfying

$$-s(i) = c_1 s(i-1) + c_2 s(i-2) + \cdots + c_l s(i-l) \ \text{ for all } l \leq i < L$$

The polynomial $c(x) = c_0 + c_1 x + \cdots + c_l x^l$ is called a minimal polynomial of $\{s(n)\}$. Let $\{s(n)\}$ be a sequence of period L over a field F, and $S(x) = s(0) + s(1)x + \cdots + s(L-1)x^{L-1}$. It is well known that[3]

1. the mimimal polynomial of $\{s(n)\}$ is given by

$$c(x) = (x^L - 1)/\gcd(x^L - 1, S(x))$$

2. the linear complexity of $\{s(n)\}$ is given by

$$C_L = L - \deg(\gcd(x^L - 1, S(x)))$$

Lemma 1. *For $a \in Z^*_{p^3}$ and $1 \leq i \leq 3$*

$$aD_0^{(p^i)} = \begin{cases} D_0^{(p^i)}, & \text{if } a \in D_0^{(p^i)} \\ D_1^{(p^i)}, & \text{if } a \in D_1^{(p^i)} \end{cases}, \quad aD_1^{(p^i)} = \begin{cases} D_1^{(p^i)}, & \text{if } a \in D_0^{(p^i)} \\ D_0^{(p^i)}, & \text{if } a \in D_1^{(p^i)} \end{cases}.$$

Proof. It can be proved in the same way as [4].

Lemma 2. *Let b be any integer. Then $D_i^{(p^3)} + bp = D_i^{(p^3)}$ and $D_i^{(p^2)} + bp = D_i^{(p^2)}$ for $i = 0, 1$.*

Proof. It can also be proved in the same way as [4].

Lemma 3. *$-1 \pmod{p^3} \in D_0^{(p^3)}$ if and only if $-1 \pmod{p^2} \in D_0^{(p^2)}$ if and only if $-1 \pmod{p} \in D_0^{(p)}$ if and only if $p \equiv 1 \pmod 4$.*

Proof. It is well known that $-1 \pmod{p} \in D_0^{(p)}$ if and only if $p \equiv 1 \pmod 4$[2]. Using Lemma 2, we can show $-1 \pmod{p} \in D_0^{(p)}$ implies $-1 \pmod{p^2} \in D_0^{(p^2)}$ and $-1 \pmod{p^3} \in D_0^{(p^3)}$. The converse is obvious.

Lemma 4. *$2 \in D_i^{(p^3)}$ if and only if $2 \in D_i^{(p^2)}$ if and only if $2 \in D_i^{(p)}$ for $i = 0, 1$.*

Proof. It can be proved in the same way as [4].

Let m be the order of 2 modulo p^3 and θ a primitive p^3th root of unity in $GF(2^m)$. Define

$$S(x) = \sum_{i \in C_1} x^i = 1 + \Big(\sum_{i \in D_1^{(p^3)}} + \sum_{i \in pD_1^{(p^2)}} + \sum_{i \in p^2 D_1^{(p)}}\Big) x^i \in GF(2)[x].$$

Then $S(x)$ is generating function of the prime cube sequence $\{s(n)\}$ defined before. To compute $S(\theta)$, we use the generalized cyclotomic numbers of order 2 with respect to p^i for $i \geq 1$ defined by

$$(i,j)_{p^k} = |(D_i^{(p^k)} + 1) \cap D_j^{(p^k)}| \quad i, j = 0, 1, \text{ and } k = 0, 1, 2. \tag{2}$$

Lemma 5. *[1] If $p \equiv 3 \pmod 4$, then*

$$(1,0)_{p^k} = (0,0)_{p^k} = (1,1)_{p^k} = \frac{p^{k-1}(p-3)}{4}, \text{ and } (0,1)_{p^k} = \frac{p^{k-1}(p+1)}{4}.$$

If $p \equiv 1 \pmod 4$, then

$$(0,1)_{p^k} = (1,0)_{p^k} = (1,1)_{p^k} = \frac{p^{k-1}(p-1)}{4}, \text{ and } (0,0)_{p^k} = \frac{p^{k-1}(p-5)}{4}.$$

Note that

$$0=\theta^{p^3}-1=(\theta^{p^2})^p-1=(\theta^{p^2}-1)(1+\theta^{p^2}+\theta^{2p^2}+\cdots+\theta^{(p-1)p^2}). \tag{3}$$

It follows that

$$1+\theta^{p^2}+\theta^{2p^2}+\cdots+\theta^{(p-1)p^2}=1+\sum_{i\in p^2D_0^{(p)}}\theta^i+\sum_{i\in p^2D_1^{(p)}}\theta^i=0. \tag{4}$$

(3) can be rewritten as follows:

$$0=\theta^{p^3}-1=(\theta^p)^{p^2}-1=(\theta^p-1)(1+\theta^p+\cdots+\theta^{(p^2-1)p}).$$

It follows that

$$1+\theta^p+\cdots+\theta^{(p^2-1)p}=1+\sum_{i\in p^2D_0^{(p)}\cup p^2D_1^{(p)}\cup pD_0^{(p^2)}\cup pD_1^{(p^2)}}\theta^i=0. \tag{5}$$

From (4) and (5), we obtain

$$\sum_{i\in pD_0^{(p^2)}}\theta^i=\sum_{i\in pD_1^{(p^2)}}\theta^i. \tag{6}$$

Since $\sum_{i=0}^{p^3-1}\theta^i=0$, by (5) we obtain

$$\sum_{i\in D_0^{(p^3)}}\theta^i=\sum_{i\in D_1^{(p^3)}}\theta^i. \tag{7}$$

Assume $\theta_1=\theta^p, \theta_2=\theta^{p^2}$, then θ_1 is a primitive p^2th root of unity and θ_2 is a primitive pth root of unity in $GF(2^m)$. Define

$$t_1(\theta_1)=\sum_{i\in D_1^{(p^2)}}\theta_1^i \quad \text{and} \quad t_2(\theta_2)=\sum_{i\in D_1^{(p)}}\theta_2^i.$$

Lemma 6. *[5] $\sum_{i\in pZ_p}\theta_1^i+\sum_{i\in D_1^{(p^2)}}\theta_1^i=0$ if p is an odd prime.*

Lemma 7. *$\sum_{i\in D_0^{(p^2)}}\theta_1^i=\sum_{i\in D_1^{(p^2)}}\theta_1^i=t_1(\theta_1)=0$.*

Proof. From (4),(6) and Lemma 6, obvious.

Lemma 8. *[6] $t_2(\theta_2)\in\{0,1\}$ if and only if $2\in D_0^{(p)}$ if and only if $p\equiv\pm1 \pmod 8$*

Lemma 9. *Let the symbols be the same as before,*

$$S(\theta^a)=\begin{cases}\frac{p+1}{2} \pmod 2, & \text{if } a=0\\ S(\theta), & \text{if } a\in D_0^{(p^3)}\\ S(\theta)+1, & \text{if } a\in D_1^{(p^3)}\\ \frac{p+1}{2}+t_2(\theta_2), & \text{if } a\in pD_0^{(p^2)}\\ \frac{p-1}{2}+t_2(\theta_2), & \text{if } a\in pD_1^{(p^2)}\\ 1+t_2(\theta_2), & \text{if } a\in p^2D_0^{(p)}\\ t_2(\theta_2), & \text{if } a\in p^2D_1^{(p)}.\end{cases}$$

Proof. For the case $a = 0$, we have $S(\theta^a) = S(1) = \frac{p^3+1}{2} \equiv \frac{p+1}{2}$ (mod 2). If $a \in D_0^{(p^3)}$, by definition there is an integer s such that $a = g^{2s}$. It follows that

$$\begin{aligned} aD_1^{(p^3)} &= \{g^{2s+2t+1} | t = 0, 1, \cdots, p^2(p-1)-1\} = D_1^{(p^3)} \\ apD_1^{(p^2)} &= p\{g^{2s+2t+1} | t = 0, 1, \cdots, p(p-1)-1\} = pD_1^{(p^2)} \\ ap^2D_1^{(p)} &= p^2\{g^{2s+2t+1} | t = 0, 1, \cdots, (p-1)-1\} = p^2D_1^{(p^2)}. \end{aligned}$$

Hence

$$S(\theta^a) = 1 + (\sum_{i\in D_1^{(p^3)}} + \sum_{i\in pD_1^{(p^2)}} + \sum_{i\in p^2D_1^{(p)}})\theta^{ai} = 1 + (\sum_{i\in D_1^{(p^3)}} + \sum_{i\in pD_1^{(p^2)}} + \sum_{i\in p^2D_1^{(p)}})\theta^i = S(\theta).$$

If $a \in D_1^{(p^3)}$, then $aD_1^{(p^3)} = D_0^{(p^3)}, apD_1^{(p^2)} = pD_0^{(p^2)}, ap^2D_1^{(p)} = p^2D_0^{(p^2)}$. By (4), (6) and (7)

$$S(\theta^a) = 1 + (\sum_{i\in D_0^{(p^3)}} + \sum_{i\in pD_0^{(p^2)}} + \sum_{i\in p^2D_0^{(p)}})\theta^i = S(\theta) + 1.$$

Note that $D_1^{(p^3)}$ mod p=$D_1^{(p)}$, $|D_1^{(p^3)}| = p^2|D_1^{(p)}|$, $\theta_1^{p^2} = 1$ and $\theta_2^p = 1$.
For $a = a_1p, a_1 \in Z_{p^2}^* = D_0^{(p^2)} \cup D_1^{(p^2)}$, we have

$$\begin{aligned} S(\theta^a) &= 1 + (\sum_{i\in D_1^{(p^3)}} + \sum_{i\in pD_1^{(p^2)}} + \sum_{i\in p^2D_1^{(p)}})\theta^{ai} \\ &= 1 + \sum_{i\in D_1^{(p^3)}} \theta^{a_1pi} + \sum_{i\in pD_1^{(p^2)}} \theta^{a_1pi} + \sum_{i\in p^2D_1^{(p)}} \theta^{a_1pi} \\ &= 1 + \sum_{i\in a_1D_1^{(p^3)}} \theta_1^i + \sum_{i\in a_1D_1^{(p^2)}} \theta_2^i + \frac{p-1}{2}. \end{aligned}$$

If $a_1 \in D_0^{(p^2)}$, $a_1D_1^{(p^3)} = D_1^{(p^3)}$ and $a_1D_1^{(p^2)} = D_1^{(p^2)}$. we have

$$\begin{aligned} S(\theta^a) &= \frac{p+1}{2} + \sum_{i\in D_1^{(p^3)}} \theta_1^i + \sum_{i\in D_1^{(p^2)}} \theta_2^i = \frac{p+1}{2} + p\sum_{i\in D_1^{(p^2)}} \theta_1^i + p\sum_{i\in D_1^{(p)}} \theta_2^i \\ &= \frac{p+1}{2} + t_1(\theta_1) + t_2(\theta_2) = \frac{p+1}{2} + t_2(\theta_2). \end{aligned}$$

If $a_1 \in D_1^{(p^2)}$, $a_1D_1^{(p^3)} = D_0^{(p^3)}$ and $a_1D_1^{(p^2)} = D_0^{(p^2)}$. we have

$$\begin{aligned} S(\theta^a) &= \frac{p+1}{2} + \sum_{i\in D_0^{(p^3)}} \theta_1^i + \sum_{i\in D_0^{(p^2)}} \theta_2^i \\ &= \frac{p+1}{2} + t_1(\theta_1) + 1 + t_2(\theta_2) = \frac{p-1}{2} + t_2(\theta_2). \end{aligned}$$

For $a = a_2 p^2, a_2 \in Z_p^* = D_0^{(p)} \cup D_1^{(p)}$, we have

$$\begin{aligned} S(\theta^a) &= 1 + (\sum_{i \in D_1^{(p^3)}} + \sum_{i \in pD_1^{(p^2)}} + \sum_{i \in p^2 D_1^{(p)}})\theta^{ai} \\ &= 1 + \sum_{i \in a_2 D_1^{(p^3)}} \theta^{p^2 i} + \sum_{i \in D_1^{(p^2)}} \theta_1^{a_2 p^2 i} + \sum_{i \in D_1^{(p)}} \theta_2^{a_2 p^2 i} \\ &= 1 + \sum_{i \in a_2 D_1^{(p^3)}} \theta_2^i + \frac{p^2 - p}{2} + \frac{p-1}{2}. \end{aligned}$$

If $a_2 \in D_0^{(p)}$, $a_2 D_1^{(p^3)} = D_1^{(p^3)}$ and $a_2 D_1^{(p^2)} = D_1^{(p^2)}$. we have

$$S(\theta^a) = \frac{p^2+1}{2} + \sum_{i \in D_1^{(p^3)}} \theta_2^i = \frac{p^2+1}{2} + p^2 \sum_{i \in D_1^{(p)}} \theta_2^i = 1 + t_2(\theta_2).$$

If $a_2 \in D_1^{(p^2)}$, $a_2 D_1^{(p^3)} = D_0^{(p^3)}$ and $a_2 D_1^{(p^2)} = D_0^{(p^2)}$. we have

$$S(\theta^a) = \frac{p^2+1}{2} + \sum_{i \in D_0^{(p^3)}} \theta_2^i = \frac{p^2+1}{2} + p^2 \sum_{i \in D_0^{(p)}} \theta_2^i = t_2(\theta_2).$$

Define $d_i^{(p^3)}(x) = \prod_{a \in D_i^{(p^3)}} (x - \theta^a)$, $d_i^{(p^2)}(x) = \prod_{a \in D_i^{(p^2)}} (x - \theta_1^a)$ and $d_i^{(p)}(x) = \prod_{a \in D_i^{(p)}} (x - \theta_2^a)$, $i = 0, 1$. Then

$$x^{p^3} - 1 = (x-1) d_0^{(p)}(x) d_1^{(p)}(x) d_0^{(p^2)}(x) d_1^{(p^2)}(x) d_0^{(p^3)}(x) d_1^{(p^3)}(x).$$

Lemma 10. *$d_i^{(p)}(x), d_i^{(p^2)}(x), d_i^{(p^3)}(x) \in GF(2)[x]$ if and only if $p \equiv \pm 1$ mod 8.*

Proof. Almost the same proof in [4] can be applied . If $p \equiv \pm 1$ mod 8, from Lemma 4 and 8, $2 \in D_0^{(p)} \cap D_0^{(p^2)} \cap D_0^{(p^3)}$. Then for $i = 0, 1, 2$, we have

$$(d_i^{(p^i)}(x))^2 = \prod_{a \in D_i^{(p^i)}} x^2 - \theta^{2p^i a}) = \prod_{a \in 2D_i^{(p^i)}} (x^2 - \theta^{p^i a}) = \prod_{a \in D_i^{(p^i)}} (x^2 - \theta^{p^i a}) = d_i^{(p^i)}(x^2).$$

Thus $d_i^{(p^i)}(x) \in GF(2)[x],\ i = 0, 1, 2$. If $p \equiv \pm 3$ mod 8, from Lemma 4 and 8, $2 \in D_1^{(p)} \cap D_1^{(p^2)} \cap D_1^{(p^3)}$. Then for $i = 0, 1, 2$, we have

$$(d_i^{(p^i)}(x))^2 = \prod_{a \in D_{i+1 (mod\ 2)}^{(p^i)}} (x^2 - \theta^{p^i a}) = d_{i+1 (mod\ 2)}^{(p^i)}(x^2) \neq d_i^{(p^i)}(x^2).$$

Hence $d_i^{(p^i)}(x) \notin GF(2)[x],\ i = 0, 1, 2$.

Theorem 1. *Let p be an odd prime and $\{s(n)\}$ be a prime cube sequence of period p^3. Then the linear complexity C_L of $\{s(n)\}$ is as follows:*

$$C_L = \begin{cases} \frac{p^3+1}{2}, & \textit{if } p \equiv 1 \textit{ mod } 8 \\ p^3-1, & \textit{if } p \equiv 3 \textit{ mod } 8 \\ p^3, & \textit{if } p \equiv 5 \textit{ mod } 8 \\ \frac{p^3-1}{2}, & \textit{if } p \equiv 7 \textit{ mod } 8. \end{cases}$$

Proof. If $p \equiv 1$ mod 8, from Lemmas 8, $t_2(\theta_2) \in \{0,1\}$. Furthermore, since $2 \in D_0^{(p)} \cap D_0^{(p^2)} \cap D_0^{(p^3)}$ by Lemma 4 and 8, $S(\theta^2) = S(\theta)$. Hence, $S(\theta) \in \{0,1\}$. Applying Lemma 9, we have

$$c(x) = \frac{x^{p^3}-1}{\gcd(x^{p^3}-1, S(x))} = \begin{cases} (x-1)d_1^{(p^3)}(x)d_0^{(p^2)}(x)d_0^{(p)}(x), \text{if } (S(\theta), t_2(\theta_2)) = (0,0) \\ (x-1)d_1^{(p^3)}(x)d_1^{(p^2)}(x)d_1^{(p)}(x), \text{if } (S(\theta), t_2(\theta_2)) = (0,1) \\ (x-1)d_0^{(p^3)}(x)d_0^{(p^2)}(x)d_0^{(p)}(x), \text{if } (S(\theta), t_2(\theta_2)) = (1,0) \\ (x-1)d_0^{(p^3)}(x)d_1^{(p^2)}(x)d_1^{(p)}(x), \text{if } (S(\theta), t_2(\theta_2)) = (1,1) \end{cases}$$

It follows that $C_L = \deg(c(x)) = 1 + \frac{p^3-p^2}{2} + \frac{p^2-p}{2} + \frac{p-1}{2} = \frac{p^3+1}{2}$.

For the cases of $p \equiv 3, 5$ and 7 mod 8, we can reach easily by similar procedure with the case $p \equiv 1$ mod 8.

4 Autocorrelation

The periodic autocorrelation of a binary sequence $\{s(n)\}$ of period N is defined by $C_s(\tau) = \sum_{n=0}^{L}(-1)^{s(n+\tau)-s(n)}$ where $0 \le \tau < L$. Define $d_s(i,j;\tau) = |C_i \cap (C_j + \tau)|, \quad 0 \le \tau < L,\ i,j = 0,1$

Theorem 2. *Let p be an odd prime. Then the autocorrelation profile of the binary prime cube sequence of period p^3 which is defined at (1) is as follows:*

1. $p \equiv 1 \pmod 4$

$$C_s(\tau) = \begin{cases} p^3, & \tau = 0 \pmod{p^3} \\ p^3-p-3, & \tau \in p^2 D_0^{(p)} \\ p^3-p+1, & \tau \in p^2 D_1^{(p)} \\ p^3-p^2-p-2, & \tau \in pD_0^{(p^2)} \\ p^3-p^2-p+2, & \tau \in pD_1^{(p^2)} \\ -p^2-2, & \tau \in D_0^{(p^3)} \\ -p^2+2, & \tau \in D_1^{(p^3)} \end{cases}$$

2. $p \equiv 3 \pmod 4$

$$C_s(\tau) = \begin{cases} p^3, & \tau = 0 \pmod{p^3} \\ p^3-p-1, & \tau \in p^2 D_0^{(p)} \cup p^2 D_1^{(p)} \\ p^3-p^2-p, & \tau \in pD_0^{(p^2)} \cup pD_1^{(p^2)} \\ -p^2, & \tau \in D_0^{(p^3)} \cup D_1^{(p^3)}. \end{cases}$$

Proof. Since $C_s(\tau) = p^3 - 4d_s(1,0;\tau)$, we need to calculate $d_s(1,0;\tau)$. Note that

$$\begin{aligned} d_s(1,0;\tau) =& |C_1 \cap (C_0 + \tau)| \\ =& |C_1 \cap (p^2 D_0^{(p)} + \tau)| + |C_1 \cap (pD_0^{(p^2)} + \tau)| + |C_1 \cap (D_0^{(p^3)} + \tau)| \end{aligned} \tag{8}$$

Denote the first, the second and the third term in (8) as $A(\tau)$, $B(\tau)$ and $C(\tau)$, respectively. To begin with, we are going to compute $A(\tau)$. Note that

$$\begin{aligned} A(\tau) = |C_1 \cap (p^2 D_0^{(p)} + \tau)| = |\{0\} \cap (p^2 D_0^{(p)} + \tau)| + |p^2 D_1^{(p)} \cap (p^2 D_0^{(p)} + \tau)| \\ + |pD_1^{(p^2)} \cap (p^2 D_0^{(p)} + \tau)| + |D_1^{(p^3)} \cap (p^2 D_0^{(p)} + \tau)|. \end{aligned} \tag{9}$$

Denote the first, the second, the third and the fourth term in (9) as $A_1(\tau)$, $A_2(\tau)$, $A_3(\tau)$ and $A_4(\tau)$, respectively. Let us compute $A_1(\tau)$ first. When $\tau = 0$, $A_1(\tau) = |\{0\} \cap p^2 D_0^{(p)}| = 0$. When $\tau \in pD_i^{(p^2}$ for $i = 0,1$, by Lemma 2, any element of $p^2 D_0^{(p)} + \tau$ is an element of $pD_i^{(p^2)}$ for $i = 0,1$, respectively. Similarly, when $\tau \in D_i^{(p^3)}$ for $i = 0,1$, any element of $p^2 D_0^{(p)} + \tau$ is an element of $D_i^{(p^3)}$ for $i = 0,1$, respectively. Therefore, when $\tau \in \{0\} \cup pD_0^{(p^2)} \cup pD_1^{(p^2)} \cup D_0^{(p^3)} \cup D_1^{(p^3)}$, $A_1(\tau) = 0$. Next thing to do is to compute the value of $A_1(\tau)$ when τ belongs to the set $p^2 D_0^{(p)} \cup p^2 D_1^{(p)}$. From Lemma 1 and 3, if $p \equiv 1 \bmod 4$, $\tau \in p^2 D_i^{(p)}$ implies $-\tau \in p^2 D_i^{(p)}$ for $i = 0,1$, respectively. Hence, in this case, $A_1(\tau) = 1$ if $\tau \in p^2 D_0^{(p)}$ and $A_1(\tau) = 0$ if $\tau \in p^2 D_1^{(p)}$. Likewise if $p \equiv 1 \bmod 4$, $\tau \in p^2 D_i^{(p)}$ implies $-\tau \in p^2 D_{i+1 \bmod 2}^{(p)}$ for $i = 0,1$, respectively. Hence, $A_1(\tau) = 0$ if $\tau \in p^2 D_0^{(p)}$ and $A_1(\tau) = 1$ if $\tau \in p^2 D_1^{(p)}$. Summarizing these, we have

$$A_1(\tau) = \begin{cases} 0, \tau \in \{0\} \cup pD_0^{(p^2)} \cup pD_1^{(p^2)} \cup D_0^{(p^3)} \cup D_1^{(p^3)} \\ 1, \tau \in p^2 D_0^{(p)} \text{ and } p \equiv 1 \bmod 4 \\ 0, \tau \in p^2 D_0^{(p)} \text{ and } p \equiv 3 \bmod 4 \\ 0, \tau \in p^2 D_1^{(p)} \text{ and } p \equiv 1 \bmod 4 \\ 1, \tau \in p^2 D_1^{(p)} \text{ and } p \equiv 3 \bmod 4 \end{cases} \tag{10}$$

Next let us consider $A_2(\tau)$. Similarly $A_2(\tau) = 0$ if $\tau \in \{0\} \cup pD_0^{(p^2)} \cup pD_1^{(p^2)} \cup D_0^{(p^3)} \cup D_1^{(p^3)}$. When $\tau \in p^2 D_0^{(p)} \cup p^2 D_1^{(p)}$, $A_2(\tau) = |p^2 D_1^{(p)} \cap (p^2 D_0^{(p)} + \tau)| = |p^2 D_1^{(p)} \cap (p^2 D_0^{(p)} + p^2 a)|$ for some $a \in D_0^{(p)} \cup D_1^{(p)}$. Therefore $A_2(\tau) = |D_1^{(p)} \cap (D_0^{(p)} + a)| = |a^{-1} D_1^{(p)} \cap (a^{-1} D_0^{(p)} + 1)|$ and by Lemma 1 and the definition of the generalized cyclotomic numbers of order 2 with respect to p, we have

$$A_2(\tau) = \begin{cases} 0, & \tau \in \{0\} \cup pD_0^{(p^2)} \cup pD_1^{(p^2)} \cup D_0^{(p^3)} \cup D_1^{(p^3)} \\ (0,1)_p, & \tau \in p^2 D_0^{(p)} \\ (1,0)_p, & \tau \in p^2 D_1^{(p)} \end{cases}.$$

In the case of $A_3(\tau)$, $A_3(\tau) = 0$ if $\tau \in \{0\} \cup D_0^{(p^3)} \cup D_1^{(p^3)}$ with the same reason as $A_1(\tau)$ and $A_2(\tau)$. If $\tau \in \cup pD_0^{(p^2)} \cup pD_1^{(p^2)}$, then for $i = 0,1$, any element of $p^2D_i^{(p)}+\tau$ is a multiple of p^2 mod p^3 so that it can not be an element of $pD_1^{(p^2)}$. Thus, in these cases, $A_3(\tau)=0$. In the case of $\tau\in pD_i^{(p^2)}$ for $i=0,1$, we have $p^2D_0^{(p)}+\tau\subset pD_i^{(p^2)}$. Therefore, $A_3(\tau)=|\emptyset|=0$ if $\tau\in pD_0^{(p^2)}$ and $A_3(\tau)=|p^2D_0^{(p)}+\tau|=\frac{p-1}{2}$ if $\tau\in pD_1^{(p^2)}$. Similarly, we can compute $A_4(\tau)$. Summarizing these calculation, we have

$$A_3(\tau)=\begin{cases}0, & \tau\in Z_{p^3}\setminus pD_1^{(p^2)}\\ \frac{p-1}{2}, & \tau\in pD_1^{(p^2)}\end{cases},\quad A_4(\tau)=\begin{cases}0, & \tau\in Z_{p^3}\setminus D_1^{(p^3)}\\ \frac{p-1}{2}, & \tau\in D_1^{(p^3)}\end{cases}.$$

Combining the results of $A_1(\tau)$, $A_2(\tau)$, $A_3(\tau)$ and $A_4(\tau)$, we have

$$A(\tau)=\sum_{1\le i\le 4}A_i(\tau)=\begin{cases}0, & \tau=0\\ \frac{p+3}{4}, & \tau\in p^2D_0^{(p)} \text{ and } p\equiv 1 \bmod 4\\ \frac{p+1}{4}, & \tau\in p^2D_0^{(p)} \text{ and } p\equiv 3 \bmod 4\\ \frac{p-1}{4}, & \tau\in p^2D_1^{(p)} \text{ and } p\equiv 1 \bmod 4\\ \frac{p+1}{4}, & \tau\in p^2D_1^{(p)} \text{ and } p\equiv 3 \bmod 4\\ 0, & \tau\in pD_0^{(p^2)}\\ \frac{p-1}{2}, & \tau\in pD_1^{(p^2)}\\ 0, & \tau\in D_0^{(p^3)}\\ \frac{p-1}{2}, & \tau\in D_1^{(p^3)}\end{cases} \tag{11}$$

Next we are going to compute $B(\tau)$ and $C(\tau)$. Note that

$$\begin{aligned}B(\tau)=&|\{0\}\cap(pD_0^{(p^2)}+\tau)|+|p^2D_1^{(p)}\cap(pD_0^{(p^2)}+\tau)|\\&+|pD_1^{(p^2)}\cap(pD_0^{(p^2)}+\tau)|+|D_1^{(p^3)}\cap(pD_0^{(p^2)}+\tau)|.\end{aligned} \tag{12}$$

$$\begin{aligned}C(\tau)=&|\{0\}\cap(D_0^{(p^3)}+\tau)|+|p^2D_1^{(p)}\cap(D_0^{(p^3)}+\tau)|\\&+|pD_1^{(p^2)}\cap(D_0^{(p^3)}+\tau)|+|D_1^{(p^3)}\cap(D_0^{(p^3)}+\tau)|.\end{aligned} \tag{13}$$

Denote the first, the second, the third and the fourth term in (12) as $B_1(\tau)$, $B_2(\tau)$, $B_3(\tau)$ and $B_4(\tau)$, respectively. Likewise denote the first, the second, the third and the fourth term in (13) as $C_1(\tau)$, $C_2(\tau)$, $C_3(\tau)$ and $C_4(\tau)$, respectively. With almost the same way, we can reach the following:

$p\equiv 1 \bmod 4$	$B_1(\tau)$	$B_2(\tau)$	$B_3(\tau)$	$B_4(\tau)$	$B(\tau)$
$\tau\in pD_0^{(p^2)}$	1	$\frac{p-1}{2}$	$(0,1)_{p^2}$	0	$\frac{p^2+p+2}{4}$
$\tau\in pD_1^{(p^2)}$	0	0	$(1,0)_{p^2}$	0	$\frac{p(p-1)}{4}$
$\tau\in D_1^{(p^3)}$	0	0	0	$\frac{p^2-p}{2}$	$\frac{p^2-p}{2}$
otherwise	0	0	0	0	0

(14)

$p \equiv 3 \bmod 4$	$B_1(\tau)$	$B_2(\tau)$	$B_3(\tau)$	$B_4(\tau)$	$B(\tau)$
$pD_0^{(p^2)}$	0	0	$(0,1)_{p^2}$	0	$\frac{p(p+1)}{4}$
$\tau \in pD_1^{(p^2)}$	1	$\frac{p-1}{2}$	$(1,0)_{p^2}$	0	$\frac{p^2-p+2}{4}$
$\tau \in D_1^{(p^3)}$	0	0	0	$\frac{p^2-p}{2}$	$\frac{p^2-p}{2}$
otherwise	0	0	0	0	0

(15)

By doing the same procedure repeatedly, we can reach the following:

$p \equiv 1 \bmod 4$	$C_1(\tau)$	$C_2(\tau)$	$C_3(\tau)$	$C_4(\tau)$	$C(\tau)$
$\tau \in D_0^{(p^3)}$	1	$\frac{p-1}{2}$	$\frac{p^2-p}{2}$	$(0,1)_{p^3}$	$\frac{p^3+p^2+2}{4}$
$\tau \in D_1^{(p^3)}$	0	0	0	$(1,0)_{p^3}$	$\frac{p^3-p^2}{4}$
otherwise	0	0	0	0	0

$p \equiv 3 \bmod 4$	$C_1(\tau)$	$C_2(\tau)$	$C_3(\tau)$	$C_4(\tau)$	$C(\tau)$
$\tau \in D_0^{(p^3)}$	0	0	0	$(0,1)_{p^3}$	$\frac{p^3+p^2}{4}$
$\tau \in D_1^{(p^3)}$	1	$\frac{p-1}{2}$	$\frac{p^2-p}{2}$	$(1,0)_{p^3}$	$\frac{p^3-p^2+2}{4}$
otherwise	0	0	0	0	0

(16)

Combining (11),(14), and (16), we can compute $d_s(1,0;\tau)$. Since $C_s(\tau) = p^3 - 4d_s(1,0;\tau)$, it completes the proof.

References

1. Ding, C., Helleseth, T.: New Generalized Cyclotomy and Its Application. Finite Fields and Their Applications 4, 140–166 (1998)
2. Burton, D.M.: Elementary Number Theory, 4th edn. McGraw-Hill, New York (1998)
3. Golomb, S.W.: Shift Register Sequences, Revised edn. Aegean Park Press, Laguna Hills (1982)
4. Ding, C.: Linear Complexity of Some Generalized Cyclotomic Sequences. Int. J. Algebra and Computation 8, 431–442 (1998)
5. Park, Y.H., Hong, D., Chun, E.: On the Linear Complexity of Some Generalized Cyclotomic Sequences. Int. J. Algebra and Computation 14, 431–439 (2004)
6. Cusick, T., Ding, C., Renvall, A.: Stream Ciphers and Number Theory. Elservier Science, Amsterdam (1998)
7. Yan, T., Sun, R., Xiao, G.: Autocorrelation and Linear Complexity of the New Generalized Cyclotomic Sequences. IEICE Trans. Fundamentals E90-A, 857–864 (2007)
8. Bai, E., Liu, X., Xiao, G.: Linear Complexity of New Generalized Cyclotomic Sequences of Order Two of Length pq. IEEE Trans. Inform. Theory 51, 1849–1853 (2005)