Information Sciences Letters

Volume 4
Issue 2 *May 2015*

Article 3

2015

Linear Complexity of Generalized Cyclotomic Binary Sequences of Length $4p^{n}$

Xuedong Dong
Dalian economic technological development zone, Liaoning, China, dongxuedong@sina.com

Information Sciences Letters
An International Journal

http://dx.doi.org/10.12785/isl/040203

Linear Complexity of Generalized Cyclotomic Binary Sequences of Length $4p^n$

*Xuedong Dong**

College of Information Engineering, Dalian University, Dalian 116622, P. R. China

Received: 16 Jan. 2015, Revised: 24 Mar. 2015, Accepted: 26 Mar. 2015
Published online: 1 May 2015

Abstract: In this paper,the four generalized cyclotomic binary sequences with period $4p^n$ are proposed. It is showed that the proposed generalized cyclotomic binary sequences have the maximal linear complexity,but do not have desirable autocorrelation properties.

Keywords: Binary sequences, Generalized cyclotomy, Linear complexity

1 Introduction

The linear complexity of a sequence is defined as the length of the shortest linear feedback shift register that can generate the sequence. A binary sequence with least period N is considered to be good in terms of linear complexity,if its linear complexity is larger than $N/2$. Sequences with high linear complexity are important for cryptographic applications [1]. C.Ding, T.Helleseth, and W.Shan determined the linear complexity of Legendre sequences which are actually based on cyclotomic classes of order two [2]. Then a generalized cyclotomy with respect to $p_1^{e_1}p_2^{e_2}\cdots p_t^{e_t}$ was introduced by Ding and Helleseth [3]. The linear complexity of generalized cyclotomic sequences of length pq was calculated by C. Ding [4] and E.Bai et al. [5], respectively.Autocorrelation and linear complexity of the generalized cyclotomic sequences of length p^2 and p^3 were considered by T.Yan et al. [6] and Y.-J.Kim et al. [7]. The linear complexity of the generalized cyclotomic sequences of length p^m was determined by T. Yan et al. [8]. This includes the sequences of length p^2 and p^3 as special cases. In [9], a new way of computing linear complexity of series of generalized cyclotomic sequences with length p^{n+1} was introduced, which was based on the polynomial of the classic cyclotomic sequences of period p. The linear complexity of the two generalized cyclotomic binary sequences of length $2p^m$ was investigated in [10,11,12, 13]. In this paper,the four generalized cyclotomic binary sequences with period $4p^n$ are proposed. It is showed that the proposed generalized cyclotomic binary sequences have the maximal linear complexity,but do not have desirable autocorrelation properties.

The rest of this article is organized as follows. In Section 2, we give generalized cyclotomic binary sequences of length $4p^n$.In Section 3, The linear complexity of generalized cyclotomic binary sequences of length $4p^n$ is derived. Finally, concluding remarks are given in Section 4.

2 Generalized cyclotomic binary sequences of length $4p^n$

In the rest of this paper we assume that p is an odd prime and q a prime power. For $0 \le s \le m-1$, let $C_s = \{s, sq, \cdots, sq^{m_s-1}\}$ be the cyclotomic coset containing s, where m_s is the smallest positive integer such that $sq^{m_s} \equiv s (\mathrm{mod} m)$.

Lemma 1.[14, p.322] *Let p be an odd prime number. If q is a primitive root modulo p^2, then q is a primitive root modulo p^k, for all positive integer k.*

Lemma 2.*If q is a primitive root modulo p^n then q is also a primitive root modulo p^{n-j} for all $j, 0 \le j \le n-1$.*

*Proof.*By Euler's theorem $q^{\varphi(p^{n-j})} \equiv 1(\mathrm{mod} p^{n-j})$. If w_j is the order of q modp^{n-j}, then $w_j|\varphi(p^{n-j})$ and $q^{w_j} \equiv 1(\mathrm{mod} p^{n-j})$,whence we get $q^{p^j w_j} \equiv 1(\mathrm{mod} p^n)$ which implies that $\varphi(p^n)|p^j w_j$. Thus $\varphi(p^{n-j})|w_j$ and therefore $\varphi(p^{n-j}) = w_j$.

* Corresponding author e-mail: dongxuedong@sina.com

Lemma 3. *If q is a primitive root modulo p^2 and $q \equiv 3(mod4)$, then the order of q modulo $4p^{n-j}$ is $\varphi(p^{n-j})$, for all $0 \le j \le n-1$.*

Lemma 4. *If q is a primitive root modulo p^2 and $q \equiv 3(mod4)$, then there is a positive integer a such that $(a,4pq) = 1, 1 < a < 4p, a \not\equiv q^k(mod4p)$, for all $0 \le k \le \varphi(p)-1$. Moreover $\{1,q,q^2,\cdots,q^{\varphi(p^{n-j})-1},a,aq,\cdots,aq^{\varphi(p^{n-j})-1}\}$ is a reduced residue system modulo $4p^{n-j}$, $\{1,q,q^2,\cdots,q^{\varphi(p^{n-j})-1}\}$ and $\{a,aq,\cdots,aq^{\varphi(p^{n-j})-1}\}$ are generalized cyclotomic classes of order two with respect to $4p^{n-j}$ for all $0 \le j \le n-1$.*

Proof. Let $q = l^t$, where l is a prime. Then $l \equiv 3(mod4)$ since $q \equiv 3(mod4)$. Thus $l^2 \equiv 1(mod4)$ and therefore $l^{\varphi(p)} \equiv 1(mod4p)$ and $q^{\varphi(p)} \equiv 1(mod4p)$. $1,q,q^2,\cdots,q^{\varphi(p)-1}$, $l,l^2,\cdots,l^{\varphi(p)-1}$ are $2\varphi(p)-1 = 2p-3$ numbers which are relatively prime to $4p$. From $\varphi(4p) = 2(p-1)$ it follows that there is a positive integer b such that $(b,4p) = 1, 1 < b < 4p, b \not\equiv q^k(mod4p), b \not\equiv l^k(mod4p)$ for all $0 \le k \le \varphi(p)-1$. If $(b,l) = 1$ then choose $b = a$ which satisfies $(a,4pq) = 1, 1 < a < 4p, a \not\equiv q^k(mod4p)$, for all $0 \le k \le \varphi(p)-1$. If $(b,l) \ne 1$ then $b = l^s a$, where $(a,l) = 1$. Obviously, $(a,4pq) = 1, 1 < a < 4p, a \not\equiv q^k(mod4p)$, for all $0 \le k \le \varphi(p)-1$. By Lemma 3 it is easy to verify that $\{1,q,q^2,\cdots,q^{\varphi(p^{n-j})-1},a,aq,\cdots, aq^{\varphi(p^{n-j})-1}\}$ is a reduced residue system modulo $4p^{n-j}$. Thus, $\{1,q,q^2,\cdots,q^{\varphi(p^{n-j})-1}\}$ and $\{a,aq,\cdots, aq^{\varphi(p^{n-j})-1}\}$ are generalized cyclotomic classes of order two with respect to $4p^{n-j}$ for all $0 \le j \le n-1$.

Theorem 1. *Suppose that q is a primitive root modulo p^2 and $q \equiv 3(mod4)$. There are $4n+3$ cyclotomic cosets modulo $4p^n$ over the field F_q given by*

$$C_0 = \{0\},\ C_{p^n} = \{p^n, p^n q\},\ C_{2p^n} = \{2p^n\}$$

and for $0 \le i \le n-1$,

$$C_{p^i} = \{p^i, p^i q, \cdots, p^i q^{\varphi(p^{n-i})-1}\},$$

$$C_{2p^i} = \{2p^i, 2p^i q, \cdots, 2p^i q^{\varphi(p^{n-i})-1}\},$$

$$C_{4p^i} = \{4p^i, 4p^i q, \cdots, 4p^i q^{\varphi(p^{n-i})-1}\},$$

$$C_{ap^i} = \{ap^i, ap^i q, \cdots, ap^i q^{\varphi(p^{n-i})-1}\},$$

where a is chosen as in Lemma 4.

Proof. (**i**) Since $q^2 \equiv 1(\mathrm{mod}4)$, so $p^n q^2 \equiv p^n(\mathrm{mod}4p^n)$ and therefore $C_{p^n} = \{p^n, p^n q\}$.

(**ii**) Since $q \equiv 1(\bmod 2)$, so $2p^n q \equiv 2p^n(\bmod 4p^n)$ and therefore $C_{2p^n} = \{2p^n\}$.

(**iii**) From Lemma 2 and $q^{\varphi(p^{n-i})} \equiv 1(\mathrm{mod}2p^{n-i})$ it follows that $2p^i q^{\varphi(p^{n-i})} \equiv 2p^i(\mathrm{mod}4p^n)$ and therefore $C_{2p^i} = \{2p^i, 2p^i q, \cdots, 2p^i q^{\varphi(p^{n-i})-1}\}$ for $0 \le i \le n-1$. Similarly $C_{4p^i} = \{4p^i, 4p^i q, \cdots,\ 4p^i q^{\varphi(p^{n-i})-1}\}$ for $0 \le i \le n-1$.

(**iv**) By Lemma 3 $q^{\varphi(p^{n-i})} \equiv 1(\mathrm{mod}4p^{n-i})$, so $p^i q^{\varphi(p^{n-i})} \equiv p^i(\bmod 4p^n)$ and therefore

$C_{p^i} = \{p^i, p^i q, \cdots,\ p^i q^{\varphi(p^{n-i})-1}\}$ for $0 \le i \le n-1$.

(**v**) Since $a(q^{\varphi(p^{n-i})} - 1) \equiv 0(\mathrm{mod}4p^{n-i})$, so $ap^i q^{\varphi(p^{n-i})} \equiv ap^i(\bmod 4p^n)$, and therefore

$C_{ap^i} = \{ap^i, ap^i q, \cdots, ap^i q^{\varphi(p^{n-i})-1}\}$ for $0 \le i \le n-1$.

Finally C_s for $s = 0, p^n, 2p^n, p^i, 2p^i, 4p^i, ap^i, 0 \le i \le n-1$ are all the cyclotomic cosets modulo $4p^n$ because $|C_0| + |C_{p^n}| + |C_{2p^n}| + \sum_{i=0}^{n-1}(|C_{p^i}| + |C_{2p^i}| + |C_{4p^i}| + |C_{ap^i}|) = 1 + 2 + 1 + 4\sum_{i=0}^{n-1}\varphi(p^{n-i}) = 4p^n$.

Denote $D_1^{(1)} = \bigcup_{i=0}^{n-1}(C_{p^i} \cup C_{2p^i}) \cup \{0\}$ and $D_0^{(1)} = Z_{4p^n} \backslash D_1^{(1)}$;

$D_1^{(2)} = \bigcup_{i=0}^{n-1}(C_{p^i} \cup C_{4p^i}) \cup \{0\}$ and $D_0^{(2)} = Z_{4p^n} \backslash D_1^{(2)}$;

$D_1^{(3)} = \bigcup_{i=0}^{n-1}(C_{ap^i} \cup C_{2p^i}) \cup \{0\}$ and $D_0^{(3)} = Z_{4p^n} \backslash D_1^{(3)}$;

$D_1^{(4)} = \bigcup_{i=0}^{n-1}(C_{ap^i} \cup C_{4p^i}) \cup \{0\}$ and $D_0^{(4)} = Z_{4p^n} \backslash D_1^{(4)}$;

For $1 \le k \le 4$, the generalized cyclotomic binary sequence $S_1^{(k)} = \{s_i^{(k)}\}$ of length $4p^n$ is then defined by

$$s_i^{(k)} = \begin{cases} 0, \text{ if } i \in D_0^{(k)}, \\ 1, \text{ if } i \in D_1^{(k)}. \end{cases} \quad (1)$$

For each k with $1 \le k \le 4, |D_1^{(k)}| = 1 + 2\sum_{i=0}^{n-1}\varphi(p^{n-i}) = 2p^n - 1$. Thus, the number of 1's and the number of 0's in the sequences defined above are respectively $2p^n - 1$ and $2p^n + 1$.

3 The linear complexity of generalized cyclotomic binary sequences of length $4p^n$

Let $S = \{s_i\}$ be a N-periodic binary sequence. The monic polynomial $f(x) = x^L + a_{L-1}x^{L-1} + \cdots + a_1 x + a_0 \in Z_2[x]$ is called the characteristic polynomial of S, if $s_{L+t} + a_{L-1}s_{L+t-1} + \cdots + a_1 s_{t+1} + a_0 s_t = 0$ holds for any $t \ge 0$. The characteristic polynomial $m(x) \in Z_2[x]$ with least degree is called the minimal polynomial of S, $N - deg(m(x))$, denoted by $L(S)$, is called the linear complexity of S. The generating polynomial of the sequence S is defined by $S(x) = s_0 + s_1 x + \cdots + s_{N-1}x^{N-1} \in Z_2[x]$. It is well-known that $m(x) = (x^N - 1)/gcd(x^N - 1, S(x))$. And the linear complexity of S is then given by $L(S) = N - deg(gcd(x^N - 1, S(x)))$.

Let e be the order of 2 modulo p^n and θ a primitive p^nth root of unity in F_{2^e}. where F_{2^e} denotes the finite field with order 2^e. In the following let $\sigma_s(x) = \sum_{j\in C_s} x^j$, we assume that q is a primitive root mod p^2, $q \equiv 3(mod4)$.

Lemma 5. *If q is a primitive root modulo p^k and θ is a primitive p^kth root of unity in F_{2^e}, then*

$$\sum_{s=0}^{\varphi(p^k)-1} \theta^{q^s} = \begin{cases} -1, & if\ k=1, \\ 0, & if\ k \geq 2. \end{cases}$$

Proof. Since $1, q, q^2, \cdots, q^{\varphi(p^k)-1}$ is a reduced residue system modulo p^k, we have

$$\sum_{s=0}^{\varphi(p^k)-1} \theta^{q^s} = \sum_{s=1}^{p^k} \theta^s - \sum_{s=1,p|s}^{p^k} \theta^s.$$

If $k = 1$, then

$$\sum_{s=1}^{\varphi(p)} \theta^{q^s} = \sum_{s=1}^{p} \theta^s - \sum_{s=1,p|s}^{p} \theta^s = \frac{\theta^p - 1}{\theta - 1} - \theta^p = 0 - 1 = -1.$$

If $k \neq 1$, then

$$\sum_{s=0}^{\varphi(p^k)-1} \theta^{q^s} = \sum_{s=1}^{p^k} \theta^s - \sum_{s=1,p|s}^{p^k} \theta^s = \frac{\theta^{p^k} - 1}{\theta - 1} - \frac{\theta^p[(\theta^p)^{p^{k-1}} - 1]}{\theta^p - 1} = 0.$$

Thus

$$\sum_{s=0}^{\varphi(p^k)-1} \theta^{q^s} = \begin{cases} -1, & \text{if } k=1, \\ 0, & \text{if } k \geq 2. \end{cases}$$

Lemma 6. *Let α be any primitive p^nth root of unity in F_{2^e}. For $0 \leq i, i' \leq n-1$,*

$$\sum_{h=0}^{\varphi(p^{n-i})-1} \alpha^{p^{i+i'}q^h} = \begin{cases} \varphi(p^{n-i}), & if\ i+i' \geq n, \\ -p^{n-i-1}, & if\ i+i' = n-1, \\ 0, & if\ i+i' < n-1. \end{cases}$$

Proof. Let $\beta = \alpha^{p^{i+i'}}$. When $i+i' \geq n$, $\beta = 1$ and therefore

$$\sum_{h=0}^{\varphi(p^{n-i})-1} \alpha^{p^{i+i'}q^h} = \varphi(p^{n-i}).$$

When $i+i' \leq n-1$, β is a primitive $p^{n-i-i'}$th root of unity. We have

$$\sum_{h=0}^{\varphi(p^{n-i})-1} \alpha^{p^{i+i'}q^h} = \sum_{h=0}^{\varphi(p^{n-i})-1} \beta^{q^h} \quad (2)$$

It is clear that $\beta^{q^h} = \beta^{q^r}$ if and only if $q^h \equiv q^r(\text{mod} p^{n-i-i'})$ if and only if $h \equiv r(\text{mod}\varphi(p^{n-i-i'}))$. Therefore, By Lemma 5 the sum in (2) is

$$\frac{\varphi(p^{n-i})}{\varphi(p^{n-i-i'})} \sum_{h=0}^{\varphi(p^{n-i-i'})-1} \beta^{q^h} = p^{i'} \sum_{h=0}^{\varphi(p^{n-i-i'})-1} \beta^{q^h}$$

$$= \begin{cases} -p^{n-i-1}, & \text{if } i+i' = n-1, \\ 0, & \text{if } i+i' < n-1. \end{cases}$$

Lemma 7. *Let θ be a primitive p^nth root of unity in F_{2^e}, $u \in \{1,2,4,a\}$, where a is chosen as in Lemma 4, $1 \leq v < p^n$ and $v = zp^{i'}$, where $(z,p) = 1$. Then*

$$\sigma_{up^i}(\theta^v) = \sum_{j\in C_{up^i}} (\theta^v)^j = \begin{cases} \varphi(p^{n-i}), if\ i+i' \geq n, \\ -p^{n-i-1}, if\ i+i' = n-1, \\ 0, if\ i+i' < n-1. \end{cases}$$

Proof. From $(u,p) = 1$ and $(z,p) = 1$ it follows that $(uz,p) = 1$. Therefore $\alpha = \theta^{uz}$ is also a primitive p^nth root of unity in F_{2^e}. By Lemma 6 we get

$$\sigma_{up^i}(\theta^v) = \sum_{j\in C_{up^i}} (\theta^v)^j = \begin{cases} \varphi(p^{n-i}), \text{if } i+i' \geq n, \\ -p^{n-i-1}, \text{if } i+i' = n-1, \\ 0, \text{if } i+i' < n-1. \end{cases}$$

Theorem 2. *The sequences defined in (1) have linear complexity $4p^n$.*

Proof. Using above notations, the generating polynomial of $S_1^{(1)}$ is

$$S_1^{(1)}(x) = 1 + \sum_{i=0}^{n-1} \sigma_{p^i}(x) + \sum_{i=0}^{n-1} \sigma_{2p^i}(x).$$

Let θ be a primitive p^nth root of unity in F_{2^e}. When $1 \leq v < p^n$, $S_1^{(1)}(\theta^v) = 1$ by Lemma 7, because our computations are performed in F_{2^e}. When $v = 0$, $S_1^{(1)}(\theta^v) = 1 + \sum_{i=0}^{n-1} \varphi(p^{n-i}) + \sum_{i=0}^{n-1} \varphi(p^{n-i}) = 1$. Thus, we have $gcd(x^{4p^n} - 1, S_1^{(1)}(x)) = gcd((x^{p^n} - 1)^4, S_1^{(1)}(x)) = gcd(x^{p^n} - 1, S_1^{(1)}(x)) = 1$ and the linear complexity of $S_1^{(1)}$ is then given by $L(S_1^{(1)}) = 4p^n - deg(gcd(x^{4p^n} - 1, S_1^{(1)}(x))) = 4p^n$. Similarly, we can prove that the linear complexity of $S_1^{(2)}$, $S_1^{(3)}$ and $S_1^{(4)}$ is $4p^n$.

Example 1. Let $p = 3, n = 2$ and $q = 11$.

(1) The sequence $\{s_i^{(1)}\}$ of length $4 \cdot 3^2 = 36$ is 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1,1.

(2)The sequence $\{s_i^{(2)}\}$ of length $4 \cdot 3^2 = 36$ is 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0,1.

(3)The sequence $\{s_i^{(3)}\}$ of length $4 \cdot 3^2 = 36$ is 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0.

(4)The sequence $\{s_i^{(4)}\}$ of length $4 \cdot 3^2 = 36$ is 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0,1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0,0.

The linear complexity of the sequences above is $4 \cdot 3^2 = 36$.

4 Concluding Remarks

In this paper, we proposed four generalized cyclotomic binary sequences of period $4p^n$. Then we showed that their linear complexity is maximal. Consequently, the four proposed sequences are good in terms of linear complexity. But the suggested construction indicates that the autocorrelation e.g. with shift $2p^n$ is bad. Essentially we have $s_{i+2p^n} = s_i + 1$. Thus, these sequences should be not secure in application for cryptography and communication.

Acknowledgment

This work was supported by the National Natural Sciences Foundation of China under Project Code 10171042 and the Research Project of Liaoning Education Bureau under Project Code L2014490.

References

[1] C.Ding, Int. J. Algebra Comput. **8**,431-442 (1998).
[2] C.Ding, T.Hellseth, W.Shan, IEEE Trans. Inform. Theory **44**, 1276-1278 (1998).
[3] C.Ding, T.Helleseth, Finite Fields Appl.**4**,467-474(1999).
[4] C.Ding, Finite Fields Appl. **3**, 159-174 (1997).
[5] E.Bai, X.Liu, G.Xiao, IEEE Trans. Inform. Theory **51**, 1849-1853 (2005).
[6] T.Yan, R.Sun, G.Xiao, IEICE Trans. Fundam. E90-A **4**, 857-864 (2007).
[7] Y.J. Kim, S.Y.Jin, H.Y.Song, In: S.Boztas, H.-F.Lu (eds.) AAECC 2007, LNCS, 4851, pp. 188-197. Springer, Heidelberg, 2007.
[8] T.Yan, S.Li, G.Xiao, Appl. Math. Lett. **21**, 187-193 (2008).
[9] E.Edemskiy, Des. Codes Cryptogr. **61**, 251-260 (2011).
[10] J.W.Zhang, C.A.Zhao, X.Ma, Appl. Algebra Eng. Commun. Comput. **21**, 93-108 (2010).
[11] L.Tan, H.Xu, W.F.Qi, Appl. Algebra Eng. Commun. Comput. **23**, 221-232 (2012).
[12] P.Ke, J.Zhang, S.Zhang, Des. Codes Cryptogr. **67**,325-339 (2013).
[13] V. Edemskiy, O. Antonova, Appl. Algebra Eng. Commun. Comput.**25**,213-223 (2014).
[14] Kenneth H.Rosen, Elementary Number Theory and Its Applications, 4th edition, Addison-Wesley,2000.

Xuedong Dong received his Ph.D degree from Nanyang Technological University in 1999. He is currently a Professor in College of Information Engineering, Dalian University. His research interests are in the areas of cryptography and coding theory. He has published about 30 research papers in journals and conferences.