Trace Representations and Multi-rate Constructions of Two Classes of Generalized Cyclotomic Sequences

Tongjiang Yan[1,2], Xiaoni Du[2,3], Shuqing Li[4], and Guozhen Xiao[2]
(Corresponding author: Tongjiang Yan)

College of Mathematics and Computational Sciences, China University of Petroleum, Dongying 257061, China.[1]
ISN National Key Laboratory, Xidian University, Xi'an 710071, China.[2]
Math. and Inform. Sci., Northwest Normal University, Lanzhou, 730070, China.[3]
Comp. and Comm. Eng., China University of Petroleum, Dongying, 257061, China.[4]
(Email: yantoji@163.com)

(Received June 28, 2006; revised Nov. 7, 2006, and accepted May 2, 2007)

Abstract

In this paper, two classes of generalized cyclotomic sequences of period pq are reconstructed by means of multi-rate parallel combinations of binary Legendre sequences which are clocked at different rates. Then these generalized cyclotomic sequences can be generated by combinations of short and cheap LFSR's. From the multi-rate constructions and the trace representation of binary Legendre sequences, we present trace representations of these generalized cyclotomic sequences, which is important to the investigation of cryptographic properties of these sequences.

Keywords: Cyclotomic sequence, linear complexity, minimal polynomial, stream cipher

1 Introduction and Preliminaries

This paper investigates the trace representations and generations of a binary Ding Generalized Cyclotomic Sequence (DGCS) and a binary Whiteman Generalized Cyclotomic Sequence (WGCS) by means of multi-rate parallel combinations of constituent binary Legendre sequences which are clocked at different rates. These combinations, proposed initially by M. G. Parker ([8]), demonstrate that sequences with large linear complexity can be generated without resorting to linear feedback shift registers (LFSR) of large length. Trace representation is an important tool in the investigation of sequences, by which we can yield some properties such as linear complexity, correlation and distribution of runs. DGCS and WGCS, introduced by C. Ding in 1998 and 1997 respectively, are interesting for their large linear complexity (larger than $\frac{pq}{2}$) and low autocorrelation ([1, 2, 4, 5, 6]). Obviously, the LFSR's to produce these sequences must be longer than $\frac{pq}{2}$. Our results show that they can be produced by modifying two LFSR's with length p and q. Section 1 introduces the DGCS and WGCS. In Section 2, Legendre sequence and its trace representation are proposed. In Sections 3 and 4, Multi-rate constructions and trace representations of DGCSs and WGCSs are obtained.

In this paper, Z_N denotes the residue ring of N, $Z_N^* = Z_N \setminus \{0\}$. GF$(N)$ is a finite field with N elements. $Tr_m^n(x)$ denotes the trace function from GF(p^m) to GF(p^n). Let F be a subset of Z_N and a be an element of Z_N. Define $aF = \{af : f \in F\}$.

2 DGCS and WGCS

Let p and q $(p < q)$ be two odd primes with $\gcd(p-1, q-1) = 2$. Define $N = pq$, $e = (p-1)(q-1)/2$. The Chinese Remainder Theorem guarantees that there exists a common primitive root g of both p and q. Then the order of g modulo N is e. Let x be an integer satisfying $x \equiv g \bmod p$, $x \equiv 1 \bmod q$. Thus we can get a subgroup of the residue ring Z_N with its multiplication ([9])

$$Z_N^* = \{g^u x^i : u = 0, 1, \cdots, e-1; i = 0, 1\}.$$

The sets

$$D_i = \{g^{2u+i} x^j : u = 0, 1, \cdots, \frac{e}{2} - 1, j = 0, 1\}$$

and

$$D_i' = \{g^u x^i ; u = 0, 1, \cdots, e-1\},$$

$i = 0, 1$, are defined as DGCs and WGCs of order 2 with respect to p and q([6, 4]) respectively.

Define

$D_i^{(p)} = \{g^{2u+i} : u = 0, 1, \cdots, \frac{p-3}{2}\},$
$D_i^{(q)} = \{g^{2u+i} : u = 0, 1, \cdots, \frac{q-3}{2}\},$
$P = \{p, 2p, \cdots, (q-1)p\},$
$Q = \{q, 2q, \cdots, (p-1)q\},$ $R = \{0\},$
$C_1 = qD_1^{(p)} \cup pD_1^{(q)} \cup D_1,$ $C_1' = P \cup D_1'.$

The binary DGCS and binary WGCS of order 2 are defined respectively as

$$s_i = \begin{cases} 1, & \text{if } i \bmod N \in C_1, \\ 0, & \text{otherwise,} \end{cases}$$

and

$$s_i = \begin{cases} 1, & \text{if } i \bmod N \in C_1', \\ 0, & \text{otherwise.} \end{cases}$$

3 Legendre Sequence and its Trace Representation

Let QR_p and QNR_p be the sets of quadratic residue and quadratic nonresidue of prime p respectively. Then $QR_p + QNR_p = Z_p^*$ and it follows that

Lemma 1. *Let the symbols be the same as before.* $D_0^{(p)} = QR_p, D_1^{(p)} = QNR_p$, $D_0^{(q)} = QR_q, D_1^{(q)} = QNR_q$.

Lemma 2. *([8]) Let* $x_0, x_1 \in QR_p, y_0, y_1 \in QNR_p$*.Then* $x_0y_0, x_1y_1 \in QNR_p$ *and* $x_0x_1, y_0y_1 \in QR_p$.

Legendre sequence $s_p(t)$ of period p is defined as follows:

$$s_p(t) = \begin{cases} 1, & \text{if } t = 0 \bmod p, \\ 1, & \text{if } t \in QNR_p, \\ 0, & \text{if } \ t \in QR_p, \\ 0, & \text{if } t \text{ is non-integer.} \end{cases}$$

The Witness Set $WS(q, n)$ is the set of all factors of $q^n - 1$ which do not occur as factors of $q^t - 1, t \mid n, t \neq n$.

Lemma 3. *([8]) The Legendre sequence* $s_p(t)$ *of prime period* p *has a minimal trace representation defined by*

$$s_p(0) = 1, s_p(t) = \sum_{i=0}^{\frac{p-1}{2v}-1} Tr_{2^a}^n(\alpha^{u^{2i}t} + \alpha^{u^{2i}k}),$$

where $k \in QR_p, t > 0$*,* α *is a* p^{th} *root of* 1*,* $p \in WS(2, n), \alpha \in GF(2^n), n = 2^a v$*,* v *is odd, and* u *is a primitive element of* Z_p*. Without loss of generality,* k *can be chosen as* 1*.*

4 Multi-rate Construction and Trace Representation of DGCS

Definition 1. *In this paper, we define*

$$s_p'(t) = \begin{cases} 0, & \textit{if } t \equiv 0 \bmod p, \\ s_p(t), & \textit{otherwise,} \end{cases}$$

and

$$\delta_p(t) = \begin{cases} 0, & \textit{if } t \equiv 0 \bmod p, \\ 1, & \textit{otherwise.} \end{cases}$$

Theorem 1. *Ding generalized cyclotomic sequence* $s(t)$ *of order* 2 *with respect to* p *and* q *can be constructed by*

$$s(0) = 0, s(t) = s_q'(t)\delta_p(t) + s_q'(\frac{t}{p}) + s_p'(\frac{t}{q}).$$

Proof. If $t \in qD_1^{(p)} \cup qD_0^{(p)}$, then $s_q'(\frac{t}{p}) = 0, s_q'(t) = 0$, and $\delta_p(t) = 1$. So $s(t) = s_p'(\frac{t}{q})$. From Lemma 1, $D_1^{(p)} = QNR_p$, $D_0^{(p)} = QR_p$. For the case $t \in qD_1^{(p)}$, we have $\frac{t}{q} \in D_1^{(p)}$. Then $\frac{t}{q} \in QNR_p$. Namely $s_p'(\frac{t}{q}) = 1$. So we have $s(t) = 1$. For the case $t \in qD_0^{(p)}$, we have $\frac{t}{q} \in D_0^{(p)}$. Then $\frac{t}{q} \in QR_p$. Namely $s_p'(\frac{t}{q}) = 0$. It follows that $s(t) = 0$.

If $t \in pD_1^{(q)} \cup pD_0^{(q)}$, then $s_p'(\frac{t}{q}) = 0$, and $\delta_p(t) = 0$. So $s(t) = s_q'(\frac{t}{p})$. From Lemma 1, we have $D_1^{(q)} = QNR_q$ and $D_0^{(q)} = QR_q$. For the case $t \in pD_1^{(q)}$, we have $\frac{t}{p} \in D_1^{(q)}$. Hence $\frac{t}{p} \in QNR_q$, and $s_q'(\frac{t}{p}) = 1$. Then $s(t) = 1$. For the case $t \in pD_0^{(q)}$, we have $\frac{t}{p} \in D_0^{(q)}$. So we have $\frac{t}{p} \in QR_q$. It follows that $s_q'(\frac{t}{p}) = 0$. Thus $s(t) = 0$.

If $t \in D_i, i = 0, 1$, then $s_q'(\frac{t}{p}) = s_p'(\frac{t}{q}) = 0$, and $\delta_p(t) = 1$. So $s(t) = s_q'(t)$, and there exists t such that $t = g^{2u+i}x^j$. Since $x \equiv 1 \bmod q, t \bmod q = g^{2u+i}x^j \bmod q = g^{2u+i} \bmod q$. For the case $i = 1$, $t \in QNR_q$. Thus $s_q'(t) = 1$. So we have $s(t) = 1$. For the case $i = 0$, we have $t \in QR_q$. Then $s_q'(t) = 0$. We get $s(t) = 0$. The theorem is proved. □

By Definition 1 and Theorem 1, we obtain the following consequence:

Theorem 2. *The trace representation of the DGCS* $s(t)$ *of order* 2 *with respect to primes* p *and* q *is given by* $s(0) = 0$ *and*

$$\begin{aligned} s(t) &= \sum_{i=0}^{\frac{q-1}{2v_q}-1} Tr_{2^{a_q}}^{n_q}[(\alpha_q^{u_q^{2i}t} + \alpha_q^{u_q^{2i}k_q})\delta_p(t) + \alpha_q^{u_q^{2i}\frac{t}{p}} \\ &\quad + \alpha_q^{u_q^{2i}k_q}] + \sum_{i=0}^{\frac{p-1}{2v_p}-1} Tr_{2^{a_p}}^{n_p}(\alpha_p^{u_p^{2i}\frac{t}{q}} + \alpha^{u_p^{2i}k_p}), \end{aligned}$$

where $k_p \in QR_p, k_q \in QR_q, t > 0$*,* α_p *and* α_q *are* p^{th} *and* q^{th} *roots of* 1 *respectively,* $p \in WS(2, n_p), q \in WS(2, n_q), \alpha_p \in GF(2^{n_p}), \alpha_q \in GF(2^{n_q}), n_p = 2^{a_p}v_p, n_q = 2^{a_q}v_q$*.* v_p, v_q *are odd, and* u_p, u_q *are primitive elements of* Z_p *and* Z_q *respectively. Without loss of generality,* k_p *and* k_q *can be chosen as* 1*.*

5 Multi-rate Construction and Trace Representation of WGCS

A Modified Jacobi sequence $\{s(t)\}$ of period pq for $t = 0, 1, 2, \cdots, pq-1$ is given by:

$$s(t) = \begin{cases} 0, & \text{if } t = 0 \bmod pq, \\ 0, & \text{if } t \in (QNR_p \cap QNR_q) \cup (QR_p \cap QR_q), \\ 1, & \text{if } t \in (QR_p \cap QNR_q) \cup (QNR_p \cap QR_q), \\ 0, & \text{if } t \not\equiv 0 \bmod p \text{ and } t \equiv 0 \bmod q, \\ 1, & \text{if } t \not\equiv 0 \bmod q \text{ and } t \equiv 0 \bmod p. \end{cases}$$

A WGCS of order 2 is actually a special case of Modified Jacobi sequences where $gcd(p-1, q-1) = 2$. The fact is proved as the following:

Since $x \equiv g \bmod p$, $x \equiv 1 \bmod q$, we have

$$g^u x^j \bmod p = g^{u+j} \bmod p, \; g^u x^j \bmod q = g^u \bmod q.$$

If $t \in D'_0$, then $t = g^u \bmod p$, which is equivalent to $t \in QNR_p \cap QNR_q$ if u is odd and $t \in QR_p \cap QR_q$ if u is even. If $t \in D'_1$, then $t = g^{u+1} \bmod p$, which is equivalent to $t \in QR_p \cap QNR_q$ if u is odd and $t \in QNR_p \cap QR_q$ if u is even. It is obvious that $t \in P$ if and only if $t \not\equiv 0 \bmod q$ and $t \equiv 0 \bmod p$, and $t \in Q$ if and only if $t \not\equiv 0 \bmod p$ and $t \equiv 0 \bmod q$.

Theorem 3. *Whiteman generalized cyclotomic sequence $s(t)$ of order 2 with respect to p and q can be constructed by the following:*

If $q \in QNR_p$ and $p \in QNR_q$, then

$$s(t) = s_p(t)\delta_p(t) + s_q(t) + s_p(\frac{t}{q}) + s_q(\frac{t}{p}).$$

If $q \in QR_p$ and $p \in QR_q$, then

$$s(t) = s_p(t) + s_q(t)\delta_q(t) + s_p(\frac{t}{q}) + s_q(\frac{t}{p}).$$

If $q \in QR_p$ and $p \in QNR_q$, then

$$s(t) = s_p(t)\delta_p(t) + s_q(t)\delta_q(t) + s_p(\frac{t}{q}) + s_q(\frac{t}{p}).$$

If $q \in QNR_p$ and $p \in QR_q$, then

$$s(t) = s_p(t) + s_q(t) + s_p(\frac{t}{q}) + s_q(\frac{t}{p}).$$

Proof. We prove only the case that $q \in QNR_p$ and $p \in QNR_q$. The other cases can be proved similarly.

It is obvious that the theorem is right for position t, $\gcd(t, pq) = 1$.

If $t \in Q$, then there exists integer k such that $t = kq$ and $\delta_p(t) = 1$, $s_q(t) = 1$, $s_q(\frac{t}{p}) = 0$, Thus

$$s(kq) = s_p(kq) + s_q(kq) + s_p(k) + s_q(\frac{kq}{p}) = s_p(kq) + s_p(k) + 1.$$

From Lemma 2, for the case $q \in QNR_p$, $s_p(kq) + s_p(k) = 1$. It follows that $s(kq) = 0$.

If $t \in P$, then there exists integer m such that $t = mp$ and $\delta_p(t) = 0$, $s_p(\frac{mp}{q}) = 0$. Thus

$$s(mp) = s_q(mp) + s_p(\frac{mp}{q}) + s_q(m) = s_q(mp) + s_q(m).$$

From Lemma 2, for the case $p \in QNR_q$, $s_q(mp) + s_q(m) = 1$. So $s(mp) = 1$. □

Lemma 3 and Theorem 3 yield the following consequence:

Theorem 4. *A Whiteman generalized cyclotomic sequence on the residue ring Z_{pq} has a trace representation as follows:*

If $q \in QNR_p$, and $p \in QNR_q$, $s(0) = 0$,

$$\begin{aligned} s(t) = \; & \textstyle\sum_{i=0}^{\frac{p-1}{2v_p}-1} Tr_{2^{a_p}}^{n_p}[(\alpha_p^{u_p^{2i}t} + \alpha_p^{u_p^{2i}k_p})\delta_p(t) \\ & +\alpha_p^{u_p^{2i}\frac{t}{q}} + \alpha_p^{u_p^{2i}k_p}] \\ & +\textstyle\sum_{i=0}^{\frac{q-1}{2v_q}-1} Tr_{2^{a_q}}^{n_q}(\alpha_q^{u_q^{2i}t} + \alpha_q^{u_q^{2i}\frac{t}{p}}). \end{aligned}$$

If $q \in QR_p$ and $p \in QR_q$, $s(0) = 0$,

$$\begin{aligned} s(t) = \; & \textstyle\sum_{i=0}^{\frac{p-1}{2v_p}-1} Tr_{2^{a_p}}^{n_p}(\alpha_p^{u_p^{2i}t} + \alpha_p^{u_p^{2i}\frac{t}{q}}) \\ & +\textstyle\sum_{i=0}^{\frac{q-1}{2v_q}-1} Tr_{2^{a_q}}^{n_q}[(\alpha_q^{u_q^{2i}t} + \alpha_q^{u_q^{2i}k_q})\delta_q(t) \\ & +\alpha_q^{u_q^{2i}\frac{t}{p}} + \alpha_q^{u_q^{2i}k_q}]. \end{aligned}$$

If $q \in QR_p$ and $p \in QNR_q$, $s(0) = 0$,

$$\begin{aligned} s(t) = \; & \textstyle\sum_{i=0}^{\frac{p-1}{2v_p}-1} Tr_{2^{a_p}}^{n_p}[(\alpha_p^{u_p^{2i}t} + \alpha_p^{u_p^{2i}k_p})\delta_p(t) \\ & +\alpha_p^{u_p^{2i}\frac{t}{q}} + \alpha_p^{u_p^{2i}k_p}] \\ & +\textstyle\sum_{i=0}^{\frac{q-1}{2v_q}-1} Tr_{2^{a_q}}^{n_q}[(\alpha_q^{u_q^{2i}t} + \alpha_q^{u_q^{2i}k_q})\delta_q(t) \\ & +\alpha_q^{u_q^{2i}\frac{t}{p}} + \alpha_q^{u_q^{2i}k_q}]. \end{aligned}$$

If $q \in QNR_p$ and $p \in QR_q$, $s(0) = 0$,

$$\begin{aligned} s(t) & = \textstyle\sum_{i=0}^{\frac{p-1}{2v_p}-1} Tr_{2^{a_p}}^{n_p}(\alpha_p^{u_p^{2i}t} + \alpha_p^{u_p^{2i}\frac{t}{q}}) \\ & \quad +\textstyle\sum_{i=0}^{\frac{q-1}{2v_q}-1} Tr_{2^{a_q}}^{n_q}(\alpha_q^{u_q^{2i}t} + \alpha_q^{u_q^{2i}\frac{t}{p}}). \end{aligned}$$

where α_p and α_q are p^{th} and q^{th} roots of 1 respectively, $p \in WS(2, n_p), q \in WS(2, n_q), \alpha_p \in GF(2^{n_p}), \alpha_q \in GF(2^{n_q}), n_p = 2^{a_p}v_p, n_q = 2^{a_q}v_q$. v_p, v_q are odd, and u_p, u_q are primitive elements of Z_p and Z_q respectively. Without loss of generality, k_p and k_q can be chosen as 1.

Remark 1. *Let $n = lcm(n_p, n_q)$, $\alpha_p = \beta^q, \alpha_q = \beta^p$, where β is a pq^{th} root of 1 in $GF(2^n)$. We can get trace representations of a DGCS and a WGCS from the extension field $GF(2^n)$.*

Remark 2. *Since a WGCS is a special Modified Jacobi sequence, the multi-rate construction and trace representation of it were actually given by other types in [7] and [3] respectively.*

Acknowledgments

This work was supported by the China University of Petroleum Doctor Foundation (Y080806) and the Science and Research Foundation (Y080803). The authors wish to thank two referees for their comments that improved the readability of this paper.

References

[1] 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. 1849-1854, 2005.

[2] E. Bai, X. Fu, and G. Xiao, "On the linear complexity of generalized cyclotomic sequences of order four over Z_{pq}," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E88-A, no. 1, pp. 392-395, 2005.

[3] Z. Dai, G. Gong, and H. Song, "Trace representation of binary Jacobi sequences," *ISIT 2003*, pp. 379, 2003.

[4] C. Ding, "Linear complexity of generalized cyclotomic binary sequence of order 2," *Finite Fields and Their Applications*, vol. 3, pp. 159-174, 1997.

[5] C. Ding, "Autocorrelation values of generalized cyclotomic sequences of order two," *IEEE Transactions on Information Theory*, vol. 44, no. 5, pp. 1699-1702, 1998.

[6] C. Ding, and T. Helleseth, "New generalized cyclotomy and its application," *Finite Fields and Their Application*, vol. 4, pp. 140-166, 1998.

[7] D. H. Green, P. R. Green, "Modified Jacobi sequences," *Computers and Digital Techniques*, vol. 147, no. 4, pp. 241-251, 2000.

[8] M. G. Parker, *Legendre and Twin-Prime Sequences: Trace and Multi-Rate Representaion*, 1999. (www.ii.uib.no/mattew/MattWeb.html)

[9] T. Storer, *Cyclotomy and Difference Set*, Chicago: Markham, 1967.

Tongjiang YAN is a lecturer of China University of Petroleum. He received his Dr. degree in cryptography from the Xidian University, Xi'an, China, in 2007. His research interests include cryptography and algebra. He has published 10 scientific papers.

Xiaoni Du is a lecturer of Northwest Normal University, Lanzhou, China. She received her M. S degree in algebra from the Lanzhou University, Lanzhou, China, in 1997. Her research interests include cryptography and algebra. She has published 10 scientific papers.

Guozhen XIAO is now a professor and Ph. D. advisor of cryptography in Xidian University, Xi'an, China. He received the M. S. degree in mathematics from the East China Normal University, Shanghai, in 1956. Now his research interests include cryptography, coding and information theory. He has published 50 scientific papers.