Chin. Ann. Math.
37B(4), 2016, 515–522
DOI: 10.1007/s11401-016-1023-z

Chinese Annals of Mathematics, Series B

On the GF(p) Linear Complexity of Hall's Sextic Sequences and Some Cyclotomic-Set-Based Sequences*

Xianmang HE[1] Liqin HU[2] Dong LI[3]

Abstract Klapper (1994) showed that there exists a class of geometric sequences with the maximal possible linear complexity when considered as sequences over $GF(2)$, but these sequences have very low linear complexities when considered as sequences over $GF(p)$ (p is an odd prime). This linear complexity of a binary sequence when considered as a sequence over $GF(p)$ is called $GF(p)$ complexity. This indicates that the binary sequences with high $GF(2)$ linear complexities are inadequate for security in the practical application, while, their $GF(p)$ linear complexities are also equally important, even when the only concern is with attacks using the Berlekamp-Massey algorithm [Massey, J. L., Shift-register synthesis and bch decoding, *IEEE Transactions on Information Theory*, **15**(1), 1969, 122–127]. From this perspective, in this paper the authors study the $GF(p)$ linear complexity of Hall's sextic residue sequences and some known cyclotomic-set-based sequences.

Keywords Linear complexity, Hall's sextic residues sequence, Cyclotomic set
2000 MR Subject Classification 94A60, 14G50, 68P25

1 Introduction

The linear complexity of a periodic sequence is an important standard to scale the randomicity of key streams, and plays an important role in the application of the sequence in cryptography and communication. The linear complexity of a periodic binary sequence is defined as the length of the shortest linear feedback shift register to generate the sequence. The periodic binary sequences with a low linear complexity (L) are not secure, since the Berlekamp-Massey algorithm (see [1]) can be used to construct the whole sequences with only $2L$ consecutive elements of the sequence.

Klapper [2] demonstrated that there exists a class of binary geometric sequences of the period $q^n - 1$ (q is a prime power p^m and p is an odd prime) with the maximal possible linear

Manuscript received December 11, 2014. Revised September 4, 2015.
[1]School of Information Science and Technology, Ningbo University, Ningbo 315122, Zhejiang, China; School of Computer Science and Technology, Fudan University, Shanghai 200433, China. E-mail: hexianmang@nbu.edu.cn
[2]Department of Mathematics, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China. E-mail: huliqin@hdu.edu.cn
[3]Information Center, National Natural Science Foundation of China, Beijing 100085, China. E-mail: lidong@nsfc.gov.cn
*This work was supported by the National Natural Science Foundation of China (Nos. 61202007, U1509213), Top Priority of the Discipline (Information and Communication Engineering) Open Foundation of Zhejiang, the Postdoctoral Science Foundation (No. 2013M540323) and the Outstanding Doctoral Dissertation in Nanjing University of Aeronautics and Astronautics (No. BCXJ 13-17).

complexity $q^n - 1$ when considered as sequences over $GF(2)$, but these sequences have very low linear complexities when applied as sequences over $GF(p)$. This pioneering work suggests that the binary sequences with high $GF(2)$ linear complexities are not necessarily cryptographically secure, since they can not prevent the attacker to get the whole sequence over $GF(p)$ whose $GF(p)$ linear complexity is low. Thus, much effort has been paid to find out ways of determining the $GF(p)$ linear complexities. Chen and Xu [3–4] proposed some constructions of the binary sequences with high $GF(2)$ linear complexities but low $GF(p)$ linear complexities, and gave some lower bounds of the $GF(p)$ linear complexities of Blum-Blum-Shub, self-shrinking, and de Bruijn sequences, etc. He has done a study of the $GF(p)$ linear complexity of Legendre sequences (see [5]).

For the cryptographic purpose, we should study the linear complexity of the binary sequence considered as a sequence over $GF(p)$, whose elements happen to be 0 or 1. Motivated by this perspective, we study the problem of the $GF(p)$ linear complexity of Hall's sextic sequences and some cyclotomic-difference-set-based sequences.

At the beginning of this paper, we present several fundamental concepts and notations that will be used in the subsequent section. Let $s(t) = s_0, s_1, \cdots, s_{N-1}$ be a sequence over a field $GF(p)$, and p is an odd prime. The linear complexity or linear span of $s(t)$ is defined to be the shortest positive integer l such that there are constants $c_0 = 1, c_1, \cdots, c_l \in GF(p)$ satisfying

$$-a_i = c_1 s_{N-1} + c_2 s_{N-2} + \cdots + c_l s_{i-l}$$

for all $l \leq i \leq n$

Such a polynomial $c(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_l x^l$ is called the feedback polynomial of the shortest linear feedback shift register (LFSR for short) that generates $s(t)$.

It is known that the feedback polynomial of $s(t)$ is given by

$$\frac{x^N - 1}{\gcd(x^N - 1, S(x))},$$

where

$$S(x) = s_0 + s_1 x + s_2 x^2 + \cdots + s_{N-1} x^{N-1}.$$

The linear complexity is calculated by

$$N - \deg(\gcd(x^N - 1, S(x))).$$

The rest of the paper is organized as follows. Section 2 will formally give the result of $GF(p)$ linear complexities of the Hall's sextic residues sequences, and the result of some cyclotomic-set-based sequences will be given in Section 3. Section 4 summarizes our results and our future work.

2 Hall's Sextic Residues Sequences

Let $N = 4u^2 + 27 = 6f + 1$ be a prime and g be a primitive root modulo N. All the nonzero elements of the integers mod N can be partitioned into six residue classes C_l, $l = 0, 1, \cdots, 5$, as

$$C_l = \{g^{6i+l} \mid i = 0, 1, \cdots, f - 1\}.$$

Hall's sextic residue sequences with respect to the period N are defined as

$$s(t) = \begin{cases} 1, & \text{if } t \in C_0 \cup C_1 \cup C_3, \\ 0, & \text{otherwise,} \end{cases}$$

where $t = 0, 1, \cdots, N-1$.

Hall's sextic residue sequences have a number of interesting properties, and we refer to [6–9] for details. Kim and Song [6] determined their $GF(2)$ linear complexity and the characteristic polynomial. The trace representation of Hall's sextic residue sequences of period $N = 7 \bmod 8$ was given in [7]. Dai etc. [8–9] explicitly described the trace representations of the binary sequences of the e-th ($e \leq 12$) power residue cyclic difference sets, including the Hall's sextic residue sequences.

For Hall's sextic residue sequences with a period N, the corresponding $S(x)$ is given by

$$S(x) = C_0(x) + C_1(x) + C_3(x).$$

Then the linear complexity of a Hall's sextic residue sequence $s(t)$ (denoted by $L_p(s)$) of the period N over $GF(p^m)$ is given by

$$L_p(s) = N - |\{j : S(\beta^j) = 0,\ 0 \leq j \leq N-1\}|, \tag{2.1}$$

where β is a primitive N-th root of unity that is the splitting field of $x^N - 1$, and m can be determined by $m = \min\{d \mid p^d = 1 \bmod N\}$.

In order to determine the linear complexity of Hall's sextic residue sequences, we need the following two lemmas.

Lemma 2.1 *With respect to the above notation, we assume further that $N = -1 \bmod p$. Let α, θ, γ be representing elements of C_0, C_1, C_2, respectively. Then*

$$S(\beta^\alpha) \cdot S(\beta^{-\alpha}) = 0, \quad S(\beta^\theta) \cdot S(\beta^{-\theta}) = 0, \quad S(\beta^\gamma) \cdot S(\beta^{-\gamma}) = 0.$$

Proof We first note that a Hall's sextic residue sequence with a period N induces a cyclic Hadamard difference set $D(v, k, \lambda)$ with parameters $v = N,\ k = \frac{N-1}{2}$ and $\lambda = \frac{N-3}{4}$ (see [10]). Consider that $(-1)^{\frac{N-1}{3}} = (-1)^{2f} = 1$ and $N = -1 \bmod 4$, so, $-1 \in C_3$. Combining with the fact that D is a (v, k, λ) difference set, we have the following equation:

$$\begin{aligned} S(\beta^\alpha) \cdot S(\beta^{-\alpha}) &= \sum_{i \in C_0 \cup C_1 \cup C_3} \beta^i \cdot \sum_{j \in C_0 \cup C_1 \cup C_3} \beta^{-j} \\ &= \sum_{i=j, i, j \in C_0 \cup C_1 \cup C_3} \beta^{i-j} + \sum_{i \neq j, i, j \in C_0 \cup C_1 \cup C_3} \beta^{i-j} \\ &= \frac{N-1}{2} + \lambda \cdot \sum_{i \in Z_N^*} \beta^i = \frac{N+1}{4}. \end{aligned}$$

Evidently, if $N = -1 \bmod p$, we have

$$S(\beta^\alpha) \cdot S(\beta^{-\alpha}) = 0.$$

Similarly, $S(\beta^\theta) \cdot S(\beta^{-\theta}) = 0$, $S(\beta^\gamma) \cdot S(\beta^{-\gamma}) = 0$, so the lemma holds.

Lemma 2.2 *With respect to the above notation, we assume again that $N = -1 \bmod p$, and then the equation*

$$(C_3(\beta) - C_0(\beta))^2 \cdot (C_4(\beta) - C_1(\beta))^2 \cdot (C_5(\beta) - C_2(\beta))^2 = 16 \bmod p$$

holds.

Lemma 2.2 can be conducted directly from the Theorem 1 in [11]. That is, $(C_3(\beta) - C_0(\beta))^2 \cdot (C_4(\beta) - C_1(\beta))^2 \cdot (C_5(\beta) - C_2(\beta))^2 = (-1)^{f+2} \cdot N \cdot M^4$. We know that the prime N can be uniquely expressed as $4N = L^2 + 27M^2$ if $N = 1 \bmod 3$. For the Hall's sextic residue sequences, $M^2 = 4$. Noting that $N = 4u^2 + 27,\ 3f = 2u^2 + 13$, f must be odd, and therefore, $(C_3(\beta) - C_0(\beta))^2 \cdot (C_4(\beta) - C_1(\beta))^2 \cdot (C_5(\beta) - C_3(\beta))^2 = (-1)^{f+3} \cdot 16 \bmod p = 16 \bmod p$.

The results of the $GF(p)$ linear complexity are stated in the following theorem.

Theorem 2.1 *Let $s(t)$ be the Hall's sextic residue sequences of the period N as before. Then the $GF(p)$ linear complexity $L_p(s)$ is given as follows:*

(1) *If $N = -1 \bmod p$, then $L_p(s) = \frac{N+1}{2}$.*

(2) *Otherwise,*

$$L_p(s) = \begin{cases} N, & S(1) \neq 0, \\ N-1, & S(1) = 0. \end{cases} \tag{2.2}$$

Proof The proof of Theorem 2.1 is then completed by considering two cases depending on whether $N = -1 \bmod p$ or not.

We first consider the case $N = -1 \bmod p$, which, according to Lemma 2.1, happens. It follows from Lemma 2.1 that $S(\beta^\alpha) \cdot S(\beta^{-\alpha}) = 0$. By Lemma 2.2, it follows that either $S(\beta^\alpha) = 0$ for all $\alpha \in C_0$, or $S(\beta^{-\alpha}) = 0$ for all $\alpha \in C_3$. Clearly, the values of $S(\beta^\alpha)$ and $S(\beta^{-\alpha})$ can not be 0 simultaneously. In this way, we can deduce that the values of $S(\beta^\theta)$ and $S(\beta^{-\theta})$ can not be 0 at the same time and that is of $S(\beta^\gamma)$ and $S(\beta^{-\gamma})$. Since $S(1) = \frac{N-1}{2}$, it follows that $S(1) = -1 \bmod p$ if $N = -1 \bmod p$. Hence, if $N = -1 \bmod p$, then by Lemma 2.1,

$$L_p(s) = N - |\{j : S(\beta^j) = 0,\ 0 \leq j \leq N-1\}| = N - \frac{N-1}{2} = \frac{N+1}{2}.$$

Secondly, we consider the case $N \neq -1 \bmod p$. By Lemma 2.1, it follows that $S(\beta^\alpha) \cdot S(\beta^{-\alpha}) = \frac{N+1}{4} \neq 0 \bmod p$, which indicates that for all $\alpha \in C_0 \cup C_3$, $S(\beta^\alpha) \neq 0$. Similarly, we have that for all $j \in C_1 \cup C_4 \cup C_2 \cup C_5$, $S(\beta^j) \neq 0$. Thus, the linear complexity $L_p(s)$ is N or $N-1$, which entirely depends on whether $S(1) \bmod p$ is 0 or not. Here, we have completed the proof of the theorem.

3 Extension to Some Known Cyclotomic Difference Sets

In this section, we discuss how we can apply Lemma 2.1 to other binary sequences based on cyclotomic difference sets. In particular, we focus on some known cyclotomic difference sets, which were described in Table 1 (see [12]). Note that the $GF(p)$ linear complexity of Legendre sequecnes has been carefully studied in [5]. Hence we focus on the following two cases: The quartic residue sequences and the 8-th power residue sequences. We omit the trivial cases for the 10-th power residue sequences, which only hold for the period $N = 31$ (see [8]).

Table 1 Some known cyclotomic difference sets

Cyclotomic ADS	Conditions	Sequences
$C_0^{(2,N)}$	$N = 1 \bmod 4$	Legendre Sequences
$C_0^{(4,N)}$	$N = 4t^2 + 1,\ t$ odd	the Quartic
$C_0^{(4,N)} \cup \{0\}$	$N = 4t^2 + 9,\ t$ odd	Residue Sequences
$C_0^{(8,N)}$	$N = 8t^2 + 1 = 64u^2 + 9,\ t, u$ odd	the 8-th Power
$C_0^{(8,N)} \cup \{0\}$	$N = 8t^2 + 49 = 64u^2 + 441,$ t odd, u even	Residue Sequences
$C_0^{(6,N)} \cup C_1^{(6,N)} \cup C_3^{(6,N)}$	$N = 4t^2 + 27,\ N = 1 \bmod 6$	Hall's Sequences

Allow us to give some notations firstly. Let $N = ef + 1$ be a prime and g be a primitive root modulo N, and all the nonzero elements of the integers can be divided into e residue classes $C_l^{(e,N)}$, $l = 0, 1, \cdots, f-1$, as

$$C_l^{(e,N)} = \{g^{e\cdot i+l} \mid i = 0, 1, \cdots, f-1\},$$

where $e = 4, 8$.

We define the quartic residue sequences and the 8-th power residue sequences as

$$s(t) = \begin{cases} 1, & t \in C_0^{(e,N)}, \\ 0, & \text{otherwise.} \end{cases} \tag{3.1}$$

With the goal of computing the $GF(p)$ linear complexity, the issue is to decide the cardinality $|\{j \mid C_0^{(e,N)}(\beta^j) = 0,\ j \in C_0 \cup C_1 \cdots \cup C_{e-1} \cup \{0\}\}|$.

3.1 The quartic residue sequences

In this subsection, Theorem 3.1 manifests our effort on the $GF(p)$ linear complexity of the quartic residue sequences, while their $GF(2)$ linear complexity was given in [8]. In the following, we denote $C_l^{(4,N)}$ as C_l for short, i.e., $C_l(x) = \sum\limits_{i \in C_l} x^i$ and $S(x) = C_0(x)$.

Theorem 3.1 *Let $s(t)$ be the quartic residue sequences of the period N, and $N = 4t^2 + 1$ (t being odd) be prime. Then the $GF(p)$ linear complexity $L_p(s)$ is given as follows:*

(1) *If $3N = -1 \bmod p$, then $L_p(s) = \frac{N+1}{2}$.*

(2) *Otherwise,*

$$L_p(s) = \begin{cases} N, & S(1) \neq 0, \\ N-1, & S(1) = 0. \end{cases} \tag{3.2}$$

Proof The quartic residue sequence with a period N induces a cyclic Hadamard difference set $D(v, k, \lambda)$ with parameters $v = N,\ k = \frac{N-1}{4}$ and $\lambda = \frac{N-5}{16}$. Consider that $(-1)^{\frac{N-1}{2}} = 1 \bmod N = 1$ and $(-1)^{\frac{N-1}{4}} = -1 \bmod N$, so, $-1 \in C_2$. Combining with the fact $-1 \in C_2$, it follows from Lemma 2.1 that $C_0(\beta)\cdot C_2(\beta) = \frac{N-1}{4} - \frac{N-5}{16} = \frac{3N+1}{16} = 0 \bmod p$ and $C_1(\beta)\cdot C_3(\beta) = \frac{3N+1}{16} = 0$.

To finish the proof, notice the fact: $(C_0(\beta) - C_2(\beta))^2 = (C_0(\beta) + C_2(\beta))^2 - 4\cdot C_0(\beta)\cdot C_2(\beta) = (C_0(\beta) + C_2(\beta))^2$, and $(C_1(\beta) - C_3(\beta))^2 = (C_1(\beta) + C_3(\beta))^2$. It follows that $(C_0(\beta) - C_2(\beta))^2 \cdot (C_1(\beta) - C_3(\beta))^2 = (C_0(\beta) + C_2(\beta))^2 \cdot (C_1(\beta) + C_3(\beta))^2$.

We observe that $C_0 \cup C_2,\ C_1 \cup C_3$ constitutes the quadratic and non-quadratic residue sets modulo N, respectively. Based on the two classical facts (see [13]): $C_0(\beta) + C_2(\beta) + C_1(\beta) + C_3(\beta) = -1$ and $(C_0(\beta) + C_2(\beta) - C_1(\beta) - C_3(\beta))^2 = (-1)^{\frac{N-1}{2}} \cdot N$, it follows that $(C_0(\beta) - C_2(\beta))^2 \cdot (C_1(\beta) - C_3(\beta))^2 = \left(\frac{N-1}{4}\right)^2 \bmod p$. We seek a contradiction to show that $\frac{N-1}{4} \neq 0 \bmod p$ under the condition $3N = -1 \bmod p$. This condition implies $p \neq 3$, indicating that $p = 3$ only happens in the second case of the theorem. If $N = 1 \bmod p$ holds, then $3N = 3 \bmod p$ and $-1 = 3 \bmod p$, which gives a contradiction. It is clear that the values of $C_0(\beta)$ and $C_2(\beta^{-1})$ can not be 0 at the same time. So are the values of $C_1(\beta)$ and $C_3(\beta)$. Moreover, $C_0(1) = \frac{N-1}{4} \neq 0 \bmod p$, that is, we prove the result. The second part of this theorem is easy to see.

3.2 The 8-th power residue sequences

In this subsection, we will present our result of the 8-th power residue sequences. Suppose that $N = 8t^2 + 1 = 64u^2 + 9 = 8f + 1$ ($t,\ u$ are odd). To simplify the description, we use C_l to denote $C_l^{(8,N)}$, and $C_l(x) = \sum_{i \in C_l} x^i$.

Now, we elaborate on the details of the Theorem 3.2.

Theorem 3.2 *Let $s(t)$ be the 8-th power residue sequences of the period N, and N be prime as before. Then on the $GF(p)$ linear complexity, $L_p(s)$ is given as follows:*

(1) *If $7N = -1 \bmod p$, then $L_p(s) = \frac{N+1}{2}$.*

(2) *Otherwise,*

$$L_p(s) = \begin{cases} N, & S(1) \neq 0, \\ N-1, & S(1) = 0. \end{cases} \tag{3.3}$$

Proof We first consider the case under the condition $7N = -1 \bmod p$. The 8-th power residue sequences guide an $\left(N, \frac{N-1}{8}, \frac{N-9}{64}\right)$-cyclic hadamard difference set. Apparently, $(-1)^{\frac{N-1}{4}} = 1 \bmod N$, while $(-1)^{\frac{N-1}{8}} = -1 \bmod N$, so, $-1 \in C_4$. Therefore, we have the following 4 equations, indicating that at least four of the total eight residue classes make $C_0(\beta^j) = 0$: $C_0(\beta) \cdot C_0(\beta^{-1}) = C_0(\beta) \cdot C_4(\beta) = \frac{N-1}{8} - \frac{N-9}{64} = \frac{7N+1}{64} = 0$, $C_1(\beta) \cdot C_5(\beta) = 0$, $C_2(\beta) \cdot C_6(\beta) = 0$, $C_3(\beta) \cdot C_7(\beta) = 0$.

For convenience, let $D_0,\ D_1,\ D_2,\ D_3$ represent $C_0 \cup C_4, C_1 \cup C_5, C_2 \cup C_6, C_3 \cup C_7$, respectively. In order to prove the final result, we need to examine the value of $(D_0(\beta) \cdot D_2(\beta)) \cdot (D_1(\beta) \cdot D_3(\beta))$. First, we compute the values of $D_0(\beta) \cdot D_2(\beta),\ D_1(\beta) \cdot D_3(\beta)$ by the cyclotomic numbers of order 4 (see [14]), respectively.

$$\begin{aligned} D_0(\beta) \cdot D_2(\beta) &= (2,0) \sum_{k \in D_0} \beta^k + (1,3) \sum_{k \in D_1} \beta^k + (0,2) \sum_{k \in D_2} \beta^k + (3,1) \sum_{k \in D_3} \beta^k \\ &= \frac{N-3+2x}{16} \cdot \sum_{k \in D_0 \cup D_2} \beta^k + \frac{N+1-2x}{16} \cdot \sum_{k \in D_1 \cup D_3} \beta^k \\ &= \frac{N-9}{16} \cdot \sum_{k \in D_0 \cup D_2} \beta^k + \frac{N+7}{16} \cdot \sum_{k \in D_1 \cup D_3} \beta^k, \end{aligned}$$

where $x = -3$ in the case of $N = 64u^2 + 9 = x^2 + 4y^2,\ x = 1 \bmod 4$.

$$\begin{aligned} D_1(\beta) \cdot D_3(\beta) &= (3,1) \sum_{k \in D_0} \beta^k + (2,0) \sum_{k \in D_1} \beta^k + (1,3) \sum_{k \in D_2} \beta^k + (0,2) \sum_{k \in D_3} \beta^k \\ &= \frac{N+7}{16} \cdot \sum_{k \in D_0 \cup D_2} \beta^k + \frac{N-9}{16} \cdot \sum_{k \in D_1 \cup D_3} \beta^k. \end{aligned}$$

Observe that

$$D_0(\beta) \cdot D_2(\beta) + D_1(\beta) \cdot D_3(\beta) = -\frac{N-1}{8}$$

and

$$(D_0(\beta) \cdot D_2(\beta) - D_1(\beta) \cdot D_3(\beta))^2 = N,$$

so

$$(D_0(\beta) \cdot D_2(\beta)) \cdot (D_1(\beta) \cdot D_3(\beta)) = \frac{(\frac{N-1}{8})^2 - N}{4} = \frac{N^2 - 10N + 1}{32}.$$

In the first case, $7N = -1 \bmod p$, which indicates that $p \neq 7$, so,

$$\frac{N^2 - 10N + 1}{32} = \frac{(-\frac{1}{7})^2 - (10 \cdot (-\frac{1}{7})) + 1}{32} = \frac{15}{392} \neq 0 \bmod p.$$

From the calculation of the value $(D_0(\beta) \cdot D_2(\beta)) \cdot (D_1(\beta) \cdot D_3(\beta))$, we know that there are four and only four of the total eight residue classes that make $C_0(\beta^j) = 0$. In addition, $C_0(\beta) = \frac{N-1}{8} = 1 \neq 0 \bmod p$. Hence, the first part of the theorem holds. The second part of this theorem can be verified easily.

4 Discussions

In this paper, we give some results on the $GF(p)$ linear complexities of Hall's sextic residue sequences, and some known cyclotomic-difference-set-based sequences. These sequences share a common feature: The $GF(p)$ linear complexity is as much as half of the sequence period N. From the view of practical use, any discussion of the $GF(2)$ linear complexity requires a discussion of the $GF(p)$ linear complexity for these binary sequences. A challenge is that the calculation of $GF(p)$ linear complexity may be as difficult as or more difficult than developing the sequences themselves.

Unfortunately, despite that the $GF(p)$ linear complexities of these known sequences have been determined, the feedback polynomial of these sequences has not been well addressed in this paper. Clearly, we are only interested in the sequences which are constructed based on the cyclic difference sets, but a plethora of sequences constructed by the cyclic almost difference sets (see [14]) or the generalized cyclotomic sequences (see [15]) on the $GF(p)$ linear complexities are still open, which will be promising directions for future work.

Acknowledgements The authors wish to thank professor Hao Chen and professor Qin Yue for their patient discussions and constructive suggestions that considerably contributed to the fulfillment of this paper.

References

[1] Massey, J. L., Shift-register synthesis and bch decoding, *IEEE Transactions on Information Theory*, **15**(1), 1969, 122–127.

[2] Klapper, A., The vulnerability of geometric sequences based on fields of odd characteristic, *Journal of Cryptology*, **7**(1), 1994, 33–51.

[3] Chen, H. and Xu, L., On the binary sequences with high $gf(2)$ linear complexities and low $gf(p)$ linear complexities, *IACR Cryptology ePrint Archive*, **2005**, 2005, 241.

[4] XU, L. Q., On $gf(p)$-linear complexities of binary sequences, *The Journal of China Universities of Posts and Telecommunications*, **16**(4), 2009. 112–124.

[5] He, X., On the $gf(p)$ linear complexity of Legendre sequences, *Journal on Communications*, **29**(3), 2008, 16–22 (in Chinese).

[6] Kim, J. H. and Song, H. Y., On the linear complexity of halls sextic residue sequences, *IEEE Transactions on Information Theory*, **47**(5), 2001, 2094–2096.

[7] Kim, J. H., Song, H. Y. and Gong, G., Trace representation of Hall's sextic residue sequences of period $p \equiv 7 \pmod 8$, Mathematical Properties of Sequences and Other Combinatorial Structures, Springer-Verlag, New York, 2003, 23–32.

[8] Dai, Z., Gong, G., Song, H. Y. and Ye, D., Trace representation and linear complexity of binary e-th power residue sequences of period, *IEEE Transactions on Information Theory*, **57**(3), 2011, 1530–1547.

[9] Dai, Z., Gong, G. and Song, H. Y., Trace representation and linear complexity of binary e-th residue sequences, Proceedings of International Workshop on Coding and Cryptography, 2003, 24–28.

[10] Baumert, L. D., Cyclic Difference Sets, Springer-Verlag, New York, 1971.

[11] Lazarus, A. J., The sextic period polynomial, *Bulletin of the Australian Mathematical Society*, **49**(2), 1994, 293–304.

[12] Colbourn, C. J. and Dinitz, J. H., Handbook of Combinatorial Designs, CRC Press, Boca Raton, 2010.

[13] Ireland, K. and Rosen, M. I., A Classical Introduction to Modern Number Theory, Springer-Verlag, Boca Raton, 1982.

[14] Ding, C., Helleseth, T. and Lam, K. Y., Several classes of binary sequences with three-level autocorrelation, *IEEE Transactions on Information Theory*, **45**(7), 1999, 2606–2612.

[15] Hu, L., Yue, Q. and Wang, M., The linear complexity of whitemans generalized cyclotomic sequences of period, *IEEE Transactions on Information Theory*, **58**(8), 2012, 5534–5543.