Journal of Applied Mathematics and Computing (2019) 59:741–751
https://doi.org/10.1007/s12190-018-1200-1

ORIGINAL RESEARCH

Trace representation of Legendre sequences over non-binary fields

Chenhuang Wu[1,2] · Chunxiang Xu[1]

Received: 6 January 2018 / Published online: 23 June 2018

Abstract
For distinct odd primes N and p, we view the N-periodic binary Legendre sequence as a p-ary sequence and present its trace representation via trace functions over $\mathbb{F}_p$. We use a skill to calculate the Mattson–Solomon polynomials of Legendre sequences and then describe the Mattson–Solomon polynomials by means of trace functions over $\mathbb{F}_p$.

Keywords Legendre sequence · Trace representation · Mattson–Solomon polynomial

Mathematics Subject Classification 94A55 · 94A60 · 65C10

1 Introduction

For an odd prime number N, the N-periodic Legendre sequence is defined as

$$s_u = \begin{cases} \frac{1+(\frac{u}{N})}{2}, & \text{if} \quad \gcd(u, N) = 1, \\ 0, & \text{otherwise}, \end{cases} \qquad u \geq 0, \tag{1}$$

where $(\frac{\cdot}{N})$ is the Legendre symbol. Let g be a (fixed) primitive root modulo N, one can define the *cyclotomic classes*

$$D_0 = \{g^{2k} \pmod{N} : 0 \leq k < (N-1)/2\}$$

✉ Chenhuang Wu
ptuwch@163.com

Chunxiang Xu
chxxu@uestc.edu.cn

1 Center for Cyber Security, School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, Sichuan, People's Republic of China

2 Provincial Key Laboratory of Applied Mathematics, Putian University, Putian 351100, Fujian, People's Republic of China

and

$$D_1 = gD_0 = \{g^{2k+1} \pmod N) : 0 \le k < (N-1)/2\}.$$

Then we get an equivalent definition of the Legendre sequence

$$s_u = \begin{cases} 0, & \text{if } u \bmod N \in D_1 \cup \{0\}, \\ 1, & \text{if } u \bmod N \in D_0, \end{cases} \quad u \ge 0. \tag{2}$$

The Legendre sequences (s_u) have been extensively studied in the literature. They have strong pseudorandomness properties: equidistribution, optimal correlation, high linear complexity, etc., see [3,4,6,9,10,14,18,23]. Aly, Winterhof [1] studied the k-error linear complexity (over $\mathbb{F}_N$) by viewing the N-periodic (s_u) as a sequence over $\mathbb{F}_N$.

In particular, for certain applications to coding theory, some binary sequences are discussed over different finite fields (not in $\mathbb{F}_2$) [7,8]. Partially motivated by the study, Wang et al considered the N-periodic Legendre sequence (s_u) in $\mathbb{F}_p$, where p is an odd prime (or a prime-power) with $\gcd(p, N) = 1$, and investigated the linear complexity and minimal polynomials over $\mathbb{F}_p$ in [11,21,22]. Certain work had actually been done by He in [13]. In this work, we will continue this project to investigate the trace representation of N-periodic Legendre sequence (s_u) in $\mathbb{F}_p$ (not in $\mathbb{F}_2$). We should remark that, the trace representation of (s_u) of Mersenne prime period and of any prime period have been described via trace functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$, where n is the order of 2 modulo N, by No et al in [19] and by Kim et al in [15], sequentially. Some special cases have been studied in [20] recently.

We will compute the *Mattson–Solomon polynomial* (see definition below) of (s_u) and present the trace representation by using trace functions over $\mathbb{F}_p$. For any N-periodic p-ary sequence (t_u), there always exists a polynomial $G(X)$ defined over finite fields of characteristic p such that

$$t_u = G(\beta^u), \quad u \ge 0,$$

where β is an Nth root of unity in an extension field of $\mathbb{F}_p$. $G(X)$ is unique if its degree is smaller than N, see [16]. Such $G(X)$ is called the *Mattson–Solomon polynomial* of (t_u) in coding theory [17]. Dai et al called $G(X)$ as a *defining polynomial* and $(G(X), \beta)$ as the *defining pair* of (t_u) in [5], where they discussed trace representation and linear complexity of certain binary sequences.

Throughout the work, we always let p be an odd prime and co-prime to N, the period of Legendre sequences.

2 Mattson–Solomon polynomials

Define polynomials

$$d_l(X) = \sum_{u \in D_l} X^u \in \mathbb{F}_p[X], \quad l = 0, 1.$$

We need the following technical lemma.

Lemma 1 *Let β be a primitive Nth root of unity in an extension field of $\mathbb{F}_p$. For any fixed pair of integers i, j with $0 \le i, j < 2$, we have*

$$d_i(\beta)d_j(\beta) + d_{i+1}(\beta)d_{j+1}(\beta) + \frac{N-1}{2} = \begin{cases} N, & \text{if } \frac{N-1}{2} + i - j \equiv 0 \pmod{2}, \\ 0, & \text{otherwise.} \end{cases}$$

Here and hereafter, the subscript of d is performed modular 2.

Proof We calculate

$$\begin{aligned} d_i(\beta)d_j(\beta) + d_{i+1}(\beta)d_{j+1}(\beta) &= \sum_{k=0}^{1} \sum_{u \in D_0} \beta^{ug^{i+k}} \sum_{v \in D_0} \beta^{vg^{j+k}} \\ &= \sum_{k=0}^{1} \sum_{u \in D_0} \beta^{ug^{i+k}} \sum_{w \in D_0} \beta^{uwg^{j+k}} \\ &\quad \text{(we use } v = uw) \\ &= \sum_{k=0}^{1} \sum_{u \in D_0} \sum_{w \in D_0} \beta^{ug^{j+k}(g^{i-j}+w)} \\ &= \sum_{w \in D_0} \sum_{k=0}^{1} \sum_{z \in D_{j+k}} \gamma_w^z \\ &\quad \left(\text{we use } z = ug^{j+k}, \gamma_w = \beta^{g^{i-j}+w}\right) \\ &= \sum_{w \in D_0} \sum_{z=1}^{N-1} \gamma_w^z. \end{aligned}$$

Let $\mathrm{ord}(\gamma_w)$ denote the order of γ_w. We note that $\mathrm{ord}(\gamma_w) | N$ since β is a primitive Nth root of unity. If $\mathrm{ord}(\gamma_w) = N$, then we have

$$\sum_{z=1}^{N-1} \gamma_w^z = \sum_{z=0}^{N-1} \gamma_w^z - 1 = \frac{1-\gamma_w^N}{1-\gamma_w} - 1 = -1 \in \mathbb{F}_p.$$

If $\mathrm{ord}(\gamma_w) = 1$, then we have

$$\sum_{z=1}^{N-1} \gamma_w^z = N - 1 \in \mathbb{F}_p.$$

Now we need to determine the number of $w \in D_0$ with $\mathrm{ord}(\gamma_w) = 1$ and the number of $w \in D_0$ with $\mathrm{ord}(\gamma_w) = N$.

We have $\mathrm{ord}(\gamma_w) = 1$ if and only if $g^{i-j} + w \equiv 0 \pmod N$, which is equivalent to $w \equiv g^{(N-1)/2+i-j} \pmod N$. This implies that $2|((N-1)/2 + i - j)$ since $w \in D_0$. That is to say, there exists an $w \in D_0$ such that $g^{i-j} + w \equiv 0 \pmod N$, which holds if and only if $2|((N-1)/2 + i - j)$. In this case w is unique. We conclude that if $2|((N-1)/2 + i - j)$, then there are $(N-1)/2 - 1$ elements $w \in D_0$ such that $\mathrm{ord}(\gamma_w) = N$ and one $w \in D_0$ such that $\mathrm{ord}(\gamma_w) = 1$, while if $2 \nmid (N-1)/2 + i - j)$, all $w \in D_0$ satisfy $\mathrm{ord}(\gamma_w) = N$.

Putting everything together, we derive

$$d_i(\beta)d_j(\beta) + d_{i+1}(\beta)d_{j+1}(\beta) = \begin{cases} \frac{N+1}{2}, & \text{if } 2|\left(\frac{N-1}{2} + i - j\right), \\ -\frac{N-1}{2}, & \text{otherwise.} \end{cases}$$

This completes the proof. □

Theorem 1 *Let β be a primitive Nth root of unity in an extension field of $\mathbb{F}_p$. Then the Mattson–Solomon polynomial of (s_u) defined in Eq. (1) or Eq. (2) is*

$$G(X) = N^{-1}\left(d_0(\beta)d_0(X) + d_1(\beta)d_1(X) + \frac{N-1}{2}\right)$$

if $N \equiv 1 \pmod 4$, and otherwise

$$G(X) = N^{-1}\left(d_0(\beta)d_1(X) + d_1(\beta)d_0(X) + \frac{N-1}{2}\right).$$

Proof We get from Lemma 1 that

$$(d_0(\beta))^2 + (d_1(\beta))^2 + \frac{N-1}{2} = \begin{cases} N, & \text{if } N \equiv 1 \pmod 4, \\ 0, & \text{if } N \equiv -1 \pmod 4, \end{cases}$$

and

$$2d_0(\beta)d_1(\beta) + \frac{N-1}{2} = \begin{cases} 0, & \text{if } N \equiv 1 \pmod 4, \\ N, & \text{if } N \equiv -1 \pmod 4. \end{cases}$$

Note that $d_i(\beta^u) = d_{i+j}(\beta)$ if $u \in D_j$, where $i, j \in \{0, 1\}$ and the subscript of d is performed modulo 2. Now, we discuss the Mattson–Solomon polynomial of (s_u).

Case 1 $N \equiv 1 \pmod 4$.

For $u \in D_0$, we have

$$\begin{aligned} G(\beta^u) &= N^{-1}\left(d_0(\beta)d_0(\beta^u) + d_1(\beta)d_1(\beta^u) + \frac{N-1}{2}\right) \\ &= N^{-1}\left((d_0(\beta))^2 + (d_1(\beta))^2 + \frac{N-1}{2}\right) \\ &= N^{-1} \cdot N = 1 = s_u. \end{aligned}$$

For $u \in D_1$, we have

$$G(\beta^u) = N^{-1}\left(d_0(\beta)d_0(\beta^u) + d_1(\beta)d_1(\beta^u) + \frac{N-1}{2}\right)$$
$$= N^{-1}\left(d_0(\beta)d_1(\beta) + d_1(\beta)d_0(\beta) + \frac{N-1}{2}\right)$$
$$= N^{-1}\left(2d_0(\beta)d_1(\beta) + \frac{N-1}{2}\right)$$
$$= N^{-1} \cdot 0 = 0 = s_u.$$

For $u = 0$, we note that

$$d_0(1) = d_1(1) = \frac{N-1}{2},$$

and

$$d_0(\beta) + d_1(\beta) = \sum_{u=1}^{N-1} \beta^u = \sum_{u=0}^{N-1} \beta^u - 1 = \frac{1-\beta^N}{1-\beta} - 1 = -1.$$

Then, we get

$$G(\beta^0) = N^{-1}\left(d_0(\beta)d_0(1) + d_1(\beta)d_1(1) + \frac{N-1}{2}\right)$$
$$= N^{-1}\left(-\frac{N-1}{2} + \frac{N-1}{2}\right) = 0 = s_u.$$

Putting everything together, we derive that

$$G(X) = N^{-1}\left(d_0(\beta)d_0(X) + d_1(\beta)d_1(X) + \frac{N-1}{2}\right)$$

is the Mattson–Solomon polynomial of (s_u) when $N \equiv 1 \pmod 4$.

Case 2 $N \equiv -1 \pmod 4$.

It can be verified in a similar way. □

Now we further consider the values of $d_0(\beta)$ and $d_1(\beta)$ in Theorem 1.

Lemma 2 *Let β be a primitive Nth root of unity in an extension field of $\mathbb{F}_p$ and p a quadratic residue class modulo N (i.e., $p \in D_0$). If N satisfies one of the following two conditions*

(1) $N \equiv 1 \pmod 4$ *and* $N \equiv 1 \pmod p$,
(2) $N \equiv -1 \pmod 4$ *and* $N \equiv -1 \pmod p$,

then we have

$$\begin{cases} d_0(\beta) = 0, \\ d_1(\beta) = -1, \end{cases} \quad \textit{or} \quad \begin{cases} d_0(\beta) = -1, \\ d_1(\beta) = 0, \end{cases}$$

and otherwise we have

$$d_0(\beta), d_1(\beta) \in \mathbb{F}_p \backslash \{0\},$$

which means that both $d_0(\beta)$ and $d_1(\beta)$ are non-zero.

Proof Firstly, we have $d_0(\beta) = d_0(\beta^p) = (d_0(\beta))^p$ since $p \in D_0$. That is to say $d_0(\beta) \in \mathbb{F}_p$. Similarly, we have $d_1(\beta) \in \mathbb{F}_p$.

For $N \equiv 1 \pmod 4$, we see that in the proof of Theorem 1

$$(d_0(\beta))^2 + (d_1(\beta))^2 = \frac{N+1}{2} = 1$$

if and only if $N \equiv 1 \pmod p$. So together with $d_0(\beta) + d_1(\beta) = -1$, we get for $N \equiv 1 \pmod p$

$$2d_0(\beta)d_1(\beta) = 0,$$

which derives that either $d_0(\beta)$ or $d_1(\beta)$ is zero. Then, it is easy to get that

$$\begin{cases} d_0(\beta) = 0, \\ d_1(\beta) = -1, \end{cases} \quad \text{or} \quad \begin{cases} d_0(\beta) = -1, \\ d_1(\beta) = 0. \end{cases}$$

For $N \equiv -1 \pmod 4$, we get similarly $2d_0(\beta)d_1(\beta) = \frac{N+1}{2} = 0$ if and only if $N \equiv -1 \pmod p$ and then the result is derived.

The proof above also tells us that

$$2d_0(\beta)d_1(\beta) \neq 0$$

for other N. □

Lemma 3 *Let β be a primitive Nth root of unity in an extension field of $\mathbb{F}_p$ and p a quadratic non-residue class modulo N (i.e., $p \in D_1$). Then both $d_0(\beta)$ and $d_1(\beta)$ are non-zero.*

Proof Since $p \in D_1$, we have for $i = 0, 1$

$$(d_i(\beta))^p = d_i(\beta^p) = d_{i+1}(\beta) = -1 - d_i(\beta),$$

which indicates both $d_0(\beta)$ and $d_1(\beta)$ are non-zero. □

From Theorem 1 and Lemmas 2 and 3, we immediately get the following results.

Theorem 2 *Let β be a primitive Nth root of unity in an extension field of $\mathbb{F}_p$, p a quadratic residue class modulo N (i.e., $p \in D_0$) and (s_u) defined in Eq.* (1) *or Eq.* (2).

(1) *For N satisfying $N \equiv 1 \pmod 4$ and $N \equiv 1 \pmod p$, if we suppose $d_0(\beta) = 0$ (of course we can also suppose $d_1(\beta) = 0$), then the Mattson–Solomon polynomial of (s_u) is*

$$G(X) = -N^{-1}d_1(X).$$

(2) *For N satisfying $N \equiv -1 \pmod 4$ and $N \equiv -1 \pmod p$, if we suppose $d_0(\beta) = 0$ (of course we can also suppose $d_1(\beta) = 0$), then the Mattson–Solomon polynomial of (s_u) is*

$$G(X) = -N^{-1}d_1(X) + N^{-1}.$$

(3) *For other N, the Mattson–Solomon polynomial of (s_u) is*

$$G(X) = N^{-1}\Big(\rho d_1(X) - (1+\rho)d_0(X) + \frac{N-1}{2}\Big).$$

where $\rho = d_0(\beta)$ and $\rho(1+\rho) \neq 0$.

Theorem 3 *Let β be a primitive Nth root of unity in an extension field of $\mathbb{F}_p$ and p a quadratic non-residue class modulo N (i.e., $p \in D_1$). Then the Mattson–Solomon polynomial of (s_u) defined in Eq.* (1) *or Eq.* (2) *is*

$$G(X) = N^{-1}\Big(\rho d_1(X) - (1+\rho)d_0(X) + \frac{N-1}{2}\Big),$$

where $\rho = d_0(\beta)$ and $\rho(1+\rho) \neq 0$.

3 Trace representation

In this section, we describe the trace representation of (s_u). For $n|m$, the trace function from finite field $\mathbb{F}_{p^m}$ to $\mathbb{F}_{p^n}$ is defined as

$$\mathrm{Tr}_n^m(X) = X + X^{p^n} + X^{p^{2n}} + \cdots + X^{p^{(m/n-1)n}}.$$

The trace functions play an important role in sequences design [12].

Theorem 4 *Let β be a primitive Nth root of unity in an extension field of $\mathbb{F}_p$, p a quadratic residue class modulo N (i.e., $p \in D_0$) and (s_u) defined in Eq.* (1) *or Eq.* (2). *Let ℓ be the order of p modulo N.*

(1) *For N satisfying* $N \equiv 1 \pmod 4$ *and* $N \equiv 1 \pmod p$, *if we suppose* $d_0(\beta) = 0$, *then the trace representation of* (s_u) *is*

$$s_u = -N^{-1} \sum_{j=0}^{\frac{N-1}{2\ell}-1} \mathrm{Tr}_1^{\ell}\left(\beta^{g^{2j+1}}\right).$$

(2) *For N satisfying* $N \equiv -1 \pmod 4$ *and* $N \equiv -1 \pmod p$, *if we suppose* $d_0(\beta) = 0$, *then the trace representation of* (s_u) *is*

$$s_u = -N^{-1} \sum_{j=0}^{\frac{N-1}{2\ell}-1} \mathrm{Tr}_1^{\ell}\left(\beta^{g^{2j+1}}\right) + N^{-1}.$$

(3) *For other N, the trace representation of* (s_u) *is*

$$s_u = N^{-1}\left(\rho \sum_{j=0}^{\frac{N-1}{2\ell}-1} \mathrm{Tr}_1^{\ell}\left(\beta^{g^{2j+1}}\right) - (1+\rho) \sum_{j=0}^{\frac{N-1}{2\ell}-1} \mathrm{Tr}_1^{\ell}\left(\beta^{ug^{2j}}\right) + \frac{N-1}{2}\right).$$

where $\rho = d_0(\beta)$ *and* $\rho(1+\rho) \neq 0$.

Proof To get the trace presentation of $s(u)$, we only need to describe $d_0(X)$ and $d_1(X)$ in Theorem 2 using trace functions.

Let U be set generated by p modulo N, i.e.,

$$U = \langle p \rangle = \{p^k \pmod N : 0 \leq k < \ell\}.$$

Since $p \in D_0$, we see that U is a subgroup of D_0 (under the multiplication). Then D_0, D_1 can be written as the union

$$D_0 = \bigcup_{k=0}^{\frac{N-1}{2\ell}-1} g^{2k}U, \quad D_1 = \bigcup_{k=0}^{\frac{N-1}{2\ell}-1} g^{2k+1}U.$$

Write polynomial

$$u(X) = \sum_{u \in U} X^u.$$

Using the fact that

$$\mathrm{Tr}_1^{\ell}(X) = X + X^p + X^{p^2} + \cdots + X^{p^{\ell-1}} \equiv u(X) \pmod{X^N - 1},$$

we derive

$$d_0(X) = \sum_{j=0}^{\frac{N-1}{2\ell}-1} u\left(X^{g^{2j}}\right) \equiv \sum_{j=0}^{\frac{N-1}{2\ell}-1} \mathrm{Tr}_1^{\ell}\left(X^{g^{2j}}\right) \pmod{X^N - 1}$$

and

$$d_1(X) = \sum_{j=0}^{\frac{N-1}{2\ell}-1} u\left(X^{g^{2j+1}}\right) \equiv \sum_{j=0}^{\frac{N-1}{2\ell}-1} \mathrm{Tr}_1^{\ell}\left(X^{g^{2j+1}}\right) \pmod{X^N - 1}.$$

Then, replacing $d_0(X)$ and $d_1(X)$ in Theorem 2 and noting that $s_u = G(\beta^u)$, we finish the proof. □

Theorem 5 *Let β be a primitive Nth root of unity in an extension field of $\mathbb{F}_p$ and p a quadratic non-residue class modulo N (i.e., $p \in D_1$). Let ℓ be the order of p modulo N. Then, the trace representation of (s_u) defined in Eq. (1) or Eq. (2) is*

$$s_u = N^{-1}\left(\rho \sum_{j=0}^{\frac{N-1}{\ell}-1} \mathrm{Tr}_2^{\ell}\left(\beta^{ug^{2j+1}}\right) - (1+\rho) \sum_{j=0}^{\frac{N-1}{\ell}-1} \mathrm{Tr}_2^{\ell}\left(\beta^{ug^{2j}}\right) + \frac{N-1}{2}\right).$$

where $\rho = d_0(\beta)$ and $\rho(1+\rho) \neq 0$.

Proof The proof is similar to that of Theorem 4. From the condition $p \in D_1$, we see that $p^2 \in D_0$ and the order of p^2 modulo N is $\frac{\ell}{2}$. We remark here that ℓ is even. Indeed, if $p \equiv g^{2k+1} \pmod N$ for some k, we get $p^{\ell} \equiv g^{(2k+1)\ell} \equiv 1 \pmod N$, which indicates that $(N-1)|\ell(2k+1)$. Then ℓ is even since $N-1$ is even.

Now write

$$V = \langle p^2 \rangle = \left\{p^{2k} \pmod N : 0 \le k < \frac{\ell}{2}\right\}.$$

Then V is a subgroup of D_0 and D_0, D_1 can be represented as

$$D_0 = \bigcup_{k=0}^{\frac{N-1}{\ell}-1} g^{2k}V, \quad D_1 = \bigcup_{k=0}^{\frac{N-1}{\ell}-1} g^{2k+1}V.$$

Similar to the proof of Theorem 4, we have

$$\mathrm{Tr}_2^{\ell}(X) = X + X^{p^2} + X^{p^{2\times 2}} + \cdots + X^{p^{2\times(\frac{\ell}{2}-1)}} \equiv v(X) \pmod{X^N - 1},$$

where $v(X) = \sum_{u \in V} X^u$. Then we describe $d_0(X)$ and $d_1(X)$ as follows

$$d_0(X) = \sum_{j=0}^{\frac{N-1}{\ell}-1} v\left(X^{g^{2j}}\right) \equiv \sum_{j=0}^{\frac{N-1}{\ell}-1} \mathrm{Tr}_2^{\ell}\left(X^{g^{2j}}\right) \pmod{X^N - 1}$$

and

$$d_1(X) = \sum_{j=0}^{\frac{N-1}{\ell}-1} v\left(X^{g^{2j+1}}\right) \equiv \sum_{j=0}^{\frac{N-1}{\ell}-1} \mathrm{Tr}_2^{\ell}\left(X^{g^{2j+1}}\right) \pmod{X^N - 1}.$$

Then, replacing $d_0(X)$ and $d_1(X)$ in Theorem 3 and noting that $s_u = G(\beta^u)$, we finish the proof. □

4 Remarks and conclusions

In this work, we view N-periodic Legendre sequences in $\mathbb{F}_2$ as in $\mathbb{F}_p$ and considered their trace representation by calculating Mattson–Solomon polynomials. The results extended the early work of No et al and Kim et al on trace representation over $\mathbb{F}_2$.

The way in this work also can be used to consider the trace representation if we put N-periodic Legendre sequences in rings, for example in $\mathbb{Z}_4$, the residue class ring modulo 4.

We finally remark that, there is a relationship between Mattson–Solomon polynomials of prime periodic sequences and their linear complexity[12, Theorem 6.3]. The *linear complexity* $LC(t_u)$ of an N-period sequence (t_u) over $\mathbb{F}_p$ is the least order L of a linear recurrence relation over $\mathbb{F}_p$

$$t_{u+L} + c_1 t_{u+L-1} + \cdots + c_{L-1} t_{u+1} + c_L t_u = 0 \quad \text{for} \quad u \geq 0,$$

where $c_1, c_2, \ldots, c_L \in \mathbb{F}_p$. By [2], $LC(t_u)$ equals the number of nonzero coefficients of the Mattson–Solomon polynomial $G(x)$ of degree $< N$. So from Theorems 2 and 3, we immediately derive the linear complexity of N-periodic Legendre sequences studied in [13,22].

Acknowledgements The work was partially supported by the National Natural Science Foundation of China under Grant Nos. 61772292, 61373140, the National Key R&D Program of China No. 2017YFB0802000, the Natural Science Foundation of Fujian Province under Grant No. 2018J01425 and 2016 Development Program for Distinguished Young Scientific Research Talent of Universities in Fujian Province.

References

1. Aly, H., Winterhof, A.: On the k-error linear complexity over $\mathbb{F}_p$ of Legendre and Sidel'nikov sequences. Des. Codes Cryptogr. **40**(3), 369–374 (2006)
2. Blahut, R.E.: Transform techniques for error control codes. IBM J. Res. Dev. **23**(3), 299–315 (1979)

3. Cusick, T.W., Ding, C., Renvall, A.: Stream Ciphers and Number Theory. Elsevier, Amsterdam (1998)
4. Damgård, I.B.: On the randomness of Legendre and Jacobi sequences. In: Advances in Cryptology CRYPTO 88, LNCS 403, pp. 163–172. Springer, New York (1988)
5. Dai, Z., Gong, G., Song, H., Ye, D.: Trace representation and linear complexity of binary e-th power residue sequences of period p. IEEE Trans. Inf. Theory **57**(3), 1530–1547 (2011)
6. Ding, C.: Pattern distributions of Legendre sequences. IEEE Trans. Inf. Theory **44**(4), 1693–1698 (1998)
7. Ding, C.: Cyclic codes from the two-prime sequences. IEEE Trans. Inf. Theory **58**(6), 3881–3891 (2012)
8. Ding, C.: Cyclic codes from cyclotomic sequences of order four. Finite Fields Appl. **23**, 8–34 (2013)
9. Ding, C., Helleseth, T., Shan, W.: On the linear complexity of Legendre sequences. IEEE Trans. Inf. Theory **44**(3), 1276–1278 (1998)
10. Edemskiy, V.: On the linear complexity of interleaved binary sequences of period 4p obtained from Hall sequences or Legendre and Hall sequences. Electron. Lett. **50**(8), 604–605 (2014)
11. Edemskiy, V., Sokolovskiy, N.: On the linear complexity of Halls sextic residue sequences over GF(q). J. Appl. Math. Comput. **54**(1–2), 297–305 (2017)
12. Golomb, S.W., Gong, G.: Signal Design for Good Correlation. Cambridge University Press, Cambridge (2005)
13. He, X.: On the $GF(p)$ linear complexity of Legendre sequence. J. Commun. **29**(3), 16–22 (2008). (in Chinese)
14. Hofer, R., Winterhof, A.: On the arithmetic autocorrelation of the Legendre sequence. Adv. Math. Commun. **11**(1), 237–244 (2017)
15. Kim, J.H., Song, H.Y.: Trace representation of Legendre sequences. Des. Codes Cryptogr. **24**(3), 343–348 (2001)
16. Massey, J.L.: Codes and ciphers: Fourier and Blahut. Kluwer International Series in Engineering and Computer Science, 105–120 (1998)
17. Mattson, H.F., Solomon, G.: A new treatment of Bose–Chaudhuri codes. J. Soc. Ind. Appl. Math. **9**(4), 654–699 (1961)
18. Mauduit, C., Sárközy, A.: On finite pseudorandom binary sequences I: measures of pseudorandomness, the Legendre symbol. Acta Arith. **82**, 365–377 (1997)
19. No, J.S., Lee, H.K., Chung, H., Song, H.Y., Yang, K.: Trace representation of Legendre sequences of Mersenne prime period. IEEE Trans. Inf. Theory **42**(6), 2254–2255 (1996)
20. Qi, M., Xiong, S., Yuan, J., Zhong, L.: A simpler trace representation of Legendre sequences. IEICE Trans. **98–A**(4), 1026–1031 (2015)
21. Wang, Q.: Linear complexity of binary cyclotomic sequences of order 6. J. Appl. Math. Comput. **49**(1), 119–125 (2015)
22. Wang, Q., Lin, D., Guang, X.: On the linear complexity of Legendre sequences over F_q. IEICE Trans. Fundam. **97**(7), 1627–1630 (2014)
23. Xiong, H., Qu, L., Li, C.: A new method to compute the 2-adic complexity of binary sequences. IEEE Trans. Inf. Theory **60**(4), 2399–2406 (2014)