IEICE TRANS. FUNDAMENTALS, VOL.E96–A, NO.9 SEPTEMBER 2013

PAPER

# New Quaternary Sequences with Ideal Autocorrelation Constructed from Legendre Sequences*

**Young-Sik KIM**[†a)], ***Member***, **Ji-Woong JANG**[††b)], ***Nonmember***, **Sang-Hyo KIM**[†††c)], ***and*** **Jong-Seon NO**[††††d)], ***Members***

**SUMMARY** In this paper, for an odd prime $p$, new quaternary sequences of even period $2p$ with ideal autocorrelation property are constructed using the binary Legendre sequences of period $p$. For the new quaternary sequences, two properties which are considered as the major characteristics of pseudo-random sequences are derived. Firstly, the autocorrelation distribution of the proposed quaternary sequences is derived and it is shown that the autocorrelation values of the proposed quaternary sequences are optimal. For both $p \equiv 1 \bmod 4$ and $p \equiv 3 \bmod 4$, we can construct optimal quaternary sequences while only for $p \equiv 3 \bmod 4$, the binary Legendre sequences can satisfy ideal autocorrelation property. Secondly, the linear complexity of the proposed quaternary sequences is also derived by counting non-zero coefficients of the discrete Fourier transform over the finite field $F_q$ which is the splitting field of $x^{2p}-1$. It is shown that the linear complexity of the quaternary sequences is larger than or equal to $p$ or $(3p+1)/2$ for $p \equiv 1 \bmod 4$ or $p \equiv 3 \bmod 4$, respectively.

***key words:*** *autocorrelation, ideal autocorrelation, legendre sequences, quaternary sequences, sequences*

## 1. Introduction

In many applications of wireless communication systems such as code division multiple access (CDMA) communication systems, pseudo-random sequences with good autocorrelation property are used to extract desired user information from the received signals. Therefore, the sequences should have low out-of-phase autocorrelation values to reduce interference and noise. If the out-of-phase autocorrelation value of a sequence is always equal to zero, then the sequence is said to have the perfect autocorrelation property. However, it is conjectured and supported by extensive simulation that there is no binary or quaternary sequence with perfect autocorrelation except for a few cases of the sequences with short period [1].

Manuscript received November 8, 2012.
Manuscript revised March 20, 2013.

[†]The author is with the Department of Information and Communication Engineering, Chosun University, Gwangju, Korea.
[††]The author is with the Faculty of Information Technology, Ulsan College, Ulsan, Korea.
[†††]The author is with the School of Information and Communication Engineering, Sungkyunkwan University, Suwon, Korea.
[††††]The author is with the Department of Electrical Engineering and Computer Science, Seoul National University, Seoul, Korea.

*This work was presented in part at IEEE ISIT'09 [12] and ISITA'12 [13].

a) E-mail: iamyskim@chosun.ac.kr
b) E-mail: stasera@gmail.com
c) E-mail: iamshkim@skku.edu
d) E-mail: jsno@snu.ac.kr

DOI: 10.1587/transfun.E96.A.1872

There have been numerous researches on binary sequences with good autocorrelation property, which include m-sequences [2], GMW sequences [3], and sequences from the images of polynomials [4], and so on. The quaternary sequences with good autocorrelation property have been also researched in [1], [5]–[9]. Sidel'nikov introduced $q$-ary sequences with good autocorrelation property, which include the quaternary sequences as a special case [5], [6]. Schotten's complementary-based sequences [1], [7], [8] have good autocorrelation for odd period. Luke, Schotten, and Hadinejad-Mahram constructed quaternary sequences with good autocorrelation [1] for even period. For period $N \equiv 2 \bmod 4$, quaternary sequences with the maximum magnitude of out-of-phase autocorrelation 2 [1] can be constructed by modifying Lee's perfect sequences [10] or by periodic multiplication method.

After some constructions are presented in [11], [12], and [20], many new quaternary sequences were found by using the inverse Gray mapping and interleaving. Tang and Ding generalized the construction in [11] and some new balanced quaternary sequences with optimal autocorrelation were found [21]. Later, Zeng et al. [25] further generalized the construction in [21]. Chung et al. proposed construction methods for quaternary sequences with three valued autocorrelation from the binary sequences with the three valued autocorrelation [24]. Yang and Ke showed that a similar approach can be applied to the binary generalized cyclotomy sequences [23], even though the constructed quaternary sequences of period $pq$ have the maximum non-trivial autocorrelation of $p-q+3$ or $\max\{q-p-1, \sqrt{5}\}$. In addition, the inverse Gray mapping construction also provided a new family of quaternary sequences with good cross-correlation property [22]. The quaternary sequences constructed using the inverse Gray mapping are compared according to their period and maximum autocorrelation values as in Table 1.

In this paper, the results on the quaternary sequence construction from Legendre sequences [12] are extended. For an odd prime $p$, new quaternary sequences of even period $2p$ with ideal autocorrelation are constructed using the Legendre sequences of period $p$. The distribution of autocorrelation values of the proposed quaternary sequences is also derived.

In cryptographic applications, the linear complexity of a sequence is considered as the most important property because it is closely related to the amount of the previous outputs in order to predict the next symbol. It is worth to know

**Table 1** Comparison of quaternary sequences constructed using the inverse Gray mapping.

| Sequences | Period | $R_{\max}$ |
|---|---|---|
| Proposed | $N = 2p$ | 2 |
| Kim-Jang-Kim-No [20] | $N \equiv 0$ or 2 mod 4 | 2 |
| Jang-Kim-Kim-No [11] | $N = 2(2^n - 1)$ | 2 |
| Tang-Ding [21] | $N \equiv 2 \bmod 4$ | 2 |
| Chung-Han-Yang [24] | $N = p^m - 1 \equiv 2 \bmod 4$ | 2 |
| | $N = p^m - 1 \equiv 0 \bmod 4$ | 4 |
| | $N = 2p(p \equiv 5 \bmod 8)$, $(p = x^2 + 4$ or $p = 1 + 4y^2)$ | 2 |
| | $N = 4(2^m - 1), 4p$, $4p(p + 2)(p, p + 2$ : prime) | 4 |
| Lim-No-Chung [22] | $N \equiv 0 \bmod 2$ | 2 |
| Zeng [25] | $N \equiv 2 \bmod 4$ | 2 |
| Yang-Ke [23] | $N = pq$ | $p - q + 3$ $q - p - 1$ $\sqrt{5}$ |

the linear complexity of the new sequences. Considering the property of the inverse Gray mapping, it is expected that the known results and approaches [17]–[19] on the linear complexity of Legendre sequences may be useful.

Firstly, Ding, Helleseth, and Shan determined the linear complexity of the binary Legendre sequences [17]. Later, Kim and Song presented a trace representation of the Legendre sequences [18]. Most recently in 2006, Aly and Winterhof determined the $k$-error linear complexity of the Legendre and Sidel'nikov sequences for some cases [19].

In this paper, we derive the linear complexity of the new quaternary sequences over the finite field $F_p$ where $p \geq 5$. From the analysis, it is shown that the linear complexity of the quaternary sequences from the binary Legendre sequences is larger than or equal to $p$ or $(3p + 1)/2$ for $p \equiv 1 \bmod 4$ or $p \equiv 3 \bmod 4$, respectively. That is, the linear complexity is greater than or equal to the half of the period $2p$. This means that with the Belerkamp-Massey algorithm, the whole sequence samples are required to figure out the next symbol of the quaternary sequences.

This paper is organized as follows; Sect. 2 presents some definitions and notations for the understanding of the following sections. In Sect. 3, we define new quaternary sequences and prove the autocorrelation properties of the proposed sequences. Then, the linear complexity of the proposed sequence is derived in Sect. 4. Finally Sect. 5 concludes this paper.

## 2. Preliminaries

Let $g(t)$ be a $q$-ary sequence of period $N$. Then a sequence $g(t)$ of period $N$ is said to be *balanced* if the difference among numbers of occurrences of each element in a period is less than or equal to one.

The autocorrelation function of $g(t)$ is defined as

$$R_g(\tau) = \sum_{t=0}^{N-1} \omega_q^{g(t)-g(t+\tau)}$$

where $0 \leq \tau < N$ and $\omega_q$ is the complex primitive $q$th root of unity, e.g., $\omega_4 = \sqrt{-1}$.

In many applications of the wireless communication systems, it is known that it is desirable for the spreading sequences to have the following properties:

- The maximum magnitude of sidelobes of their autocorrelation functions should be as low as possible;
- For the given maximum sidelobe, the number of occurrences of the maximum sidelobes is minimized.

These properties of the sequences guarantee the minimum bit error rate of CDMA systems and the minimum false alarm rate in the application of synchronization for the wireless communication systems. The sequences satisfied with the above two properties are said to have *the ideal autocorrelation property*. It is well known that the binary sequence of period $N \equiv 3 \bmod 4$ with ideal autocorrelation property has the distribution of autocorrelation values as

$$R_g(\tau) = \begin{cases} N, & \text{once} \\ -1, & N - 1 \text{ times.} \end{cases}$$

Recently, Jang, Kim, Kim, and No proposed the ideal autocorrelation property of the quaternary sequences of even period with balance property as in the following theorem.

**Theorem 1** (Jang, Kim, Kim and No [11]): For an even integer $N$, let $g(t)$ be a quaternary sequence with period $N$ and $W_g$ be the weight sum of quaternary sequence $g(t)$ defined by

$$W_g = \sum_{t=0}^{N-1} \omega_4^{g(t)}.$$

Then the autocorrelation distribution of $g(t)$ of period $N$ with ideal autocorrelation and balance property is given as

$$R_g(\tau) = \begin{cases} N, & \text{once} \\ 0, & \frac{N}{2} - 1 \text{ times} \\ -2, & \frac{N}{2} \text{ times} \end{cases} \quad (1)$$

for $W_g = 0$ and for $W_g \neq 0$

$$R_g(\tau) = \begin{cases} N, & \text{once} \\ 0, & \frac{N}{2} \text{ times} \\ -2, & \frac{N}{2} - 1 \text{ times.} \end{cases} \quad (2)$$

Let $\phi[a, b]$ be the inverse Gray mapping defined by

$$\phi[a, b] = \begin{cases} 0, & \text{if } (a, b) = (0, 0) \\ 1, & \text{if } (a, b) = (0, 1) \\ 2, & \text{if } (a, b) = (1, 1) \\ 3, & \text{if } (a, b) = (1, 0). \end{cases} \quad (3)$$

Let $a(t)$ and $b(t)$ be binary sequences of period $N$. Then a quaternary sequence $g(t) = \phi[a(t), b(t)]$ can be also expressed as [9]

$$\omega_4^{g(t)} = \frac{1+\omega_4}{2}(-1)^{a(t)} + \frac{1-\omega_4}{2}(-1)^{b(t)}. \quad (4)$$

Krone and Sarwate derived the relation between the autocorrelation functions of the binary sequences and the corresponding quaternary sequences in (4) as follows.

**Theorem 2** (Krone and Sarwate [9]): Let $a(t)$, $b(t)$, $c(t)$, and $d(t)$ be binary sequences of the same period. Let $g(t)$ and $h(t)$ be quaternary sequences defined by $g(t) = \phi[a(t), b(t)]$ and $h(t) = \phi[c(t), d(t)]$, respectively. Then the cross-correlation function $R_{gh}(\tau)$ between $g(t)$ and $h(t)$ is given as

$$R_{gh}(\tau) = \frac{1}{2}\{R_{ac}(\tau) + R_{bd}(\tau) + \omega_4(R_{ad}(\tau) - R_{bc}(\tau))\}.$$

For an odd prime $p$, let $b_0(t)$ be the binary sequence defined by

$$b_0(t) = \begin{cases} 0, & \text{for } t = 0 \\ 0, & \text{for } t \in QR \\ 1, & \text{for } t \in QNR, \end{cases} \quad (5)$$

where $QR$ and $QNR$ are the sets of quadratic residues and quadratic non-residues in the set of integers modulo $p$, $Z_p$, respectively. And let $b_1(t)$ be the binary sequence of period $p$ defined by

$$b_1(t) = \begin{cases} 1, & \text{for } t = 0 \\ 0, & \text{for } t \in QR \\ 1, & \text{for } t \in QNR \end{cases} \quad (6)$$

which corresponds to a Legendre sequence. It is easy to check that $b_k(t)$ takes the symbol $k$ one more times than the other symbol $1-k$, $k = 0, 1$, which corresponds to the balance property.

The following two definitions of the indicator function and the quadratic character are useful for expression the sequences in (5) and (6).

**Definition 3:** The indicator function is defined as

$$I(x) = \begin{cases} 1, & \text{if } x = 0 \\ 0, & \text{if } x \neq 0. \end{cases}$$

**Definition 4:** The quadratic character of $Z_p$ is defined as

$$\eta(t) = \begin{cases} 0, & \text{for } t \equiv 0 \bmod p \\ 1, & \text{for } t \in QR \\ -1, & \text{for } t \in QNR. \end{cases}$$

Then two binary sequences $b_0(t)$ and $b_1(t)$ in (5) and (6) can be represented by using the indicator function $I(x)$ and the quadratic character $\eta(t)$ of $Z_p$ as

$$(-1)^{b_k(t)} = \eta(t) + (-1)^k I(t),\ k = 0, 1. \quad (7)$$

Although the autocorrelation property of Legendre sequences was already studied [6], here we will restate it in detail for the subsequent proof of the correlation properties of the proposed quaternary sequences. Using the indicator function and the quadratic character, we can express correlation functions of two binary sequences $b_0(t)$ and $b_1(t)$ as in the following lemma.

**Lemma 5:** For an odd prime $p$, let $b_0(t)$ and $b_1(t)$ be binary sequences defined in (5) and (6), respectively. Then the correlation functions $R_{b_0}(\tau)$, $R_{b_1}(\tau)$, $R_{b_0b_1}(\tau)$, and $R_{b_1b_0}(\tau)$ are expressed as follows.

For an odd prime $p$ such that $p \equiv 1 \bmod 4$, we have

$$R_{b_0}(\tau) = \begin{cases} p, & \text{for } \tau = 0 \\ -1 + 2\eta(\tau), & \text{otherwise} \end{cases}$$

$$R_{b_1}(\tau) = \begin{cases} p, & \text{for } \tau = 0 \\ -1 - 2\eta(\tau), & \text{otherwise} \end{cases}$$

$$R_{b_0b_1}(\tau) = R_{b_1b_0}(\tau) = \begin{cases} p-2, & \text{for } \tau = 0 \\ -1, & \text{otherwise.} \end{cases}$$

For an odd prime $p$ such that $p \equiv 3 \bmod 4$, we have

$$R_{b_0}(\tau) = R_{b_1}(\tau) = \begin{cases} p, & \text{for } \tau = 0 \\ -1, & \text{otherwise} \end{cases}$$

$$R_{b_0b_1}(\tau) = \begin{cases} p-2, & \text{for } \tau = 0 \\ -1 + 2\eta(\tau), & \text{otherwise} \end{cases}$$

$$R_{b_1b_0}(\tau) = \begin{cases} p-2, & \text{for } \tau = 0 \\ -1 - 2\eta(\tau), & \text{otherwise.} \end{cases}$$

*Proof*: Since the autocorrelation of Legendre sequences is well known, what we have to derive is the cross-correlation function $R_{b_0b_1}(\tau)$ between two sequences, $b_0(t)$ and $b_1(t)$.

From (7), $b_0(t)$ and $b_1(t)$ can be rewritten as

$$(-1)^{b_0(t)} = \eta(t) + I(t) \quad (8)$$

$$(-1)^{b_1(t)} = \eta(t) - I(t). \quad (9)$$

And $R_{b_0b_1}(\tau)$ is calculated as

$$\begin{aligned} R_{b_0b_1}(\tau) &= \sum_{t=0}^{p-1} [\eta(t) + I(t)][\eta(t+\tau) - I(t+\tau)] \\ &= \sum_{t=0}^{p-1} [\eta(t)\eta(t+\tau) + I(t)\eta(t+\tau) \\ &\qquad - I(t+\tau)\eta(t) - I(t)I(t+\tau)] \\ &= \eta(\tau) - \eta(-\tau) - I(\tau) + \sum_{t=0}^{p-1} \eta(t^2 + \tau t). \end{aligned}$$

In the similar way, $R_{b_1b_0}(\tau)$ can be derived as

$$\begin{aligned} R_{b_1b_0}(\tau) &= \sum_{t=0}^{p-1} [\eta(t) - I(t)][\eta(t+\tau) + I(t+\tau)] \\ &= \sum_{t=0}^{p-1} [\eta(t)\eta(t+\tau) - I(t)\eta(t+\tau) \end{aligned}$$

$$+ I(t+\tau)\eta(t) - I(t)I(t+\tau)]$$
$$= -\eta(\tau) + \eta(-\tau) - I(\tau) + \sum_{t=0}^{p-1} \eta(t^2 + \tau t).$$

Let $N_{QR}(\tau)$ and $N_{QNR}(\tau)$ be the cardinality of the sets

$$\{t|\ t^2 + \tau t \in QR,\ 0 \le t < p\}$$
$$\{t|\ t^2 + \tau t \in QNR,\ 0 \le t < p\}$$

respectively. Then the last summation in the above $R_{b_1 b_0}(\tau)$ can be rewritten as

$$\sum_{t=0}^{p-1} \eta(t^2 + \tau t) = \begin{cases} p-1, & \tau = 0 \\ N_{QR}(\tau) - N_{QNR}(\tau) & \tau \neq 0. \end{cases}$$

Using the cyclotomic numbers of order 2 [14], it is easy to see that

$$N_{QR}(\tau) = (0,0)_2 + (0,1)_2 = \frac{p-3}{2}$$
$$N_{QNR}(\tau) = (1,0)_2 + (1,1)_2 = \frac{p-1}{2}.$$

Since $-1$ is a quadratic residue of $p$, when $p \equiv 1 \bmod 4$ and a quadratic non-residue of $p$, when $p \equiv 3 \bmod 4$, we have the followings.

For an odd prime $p$ such that $p \equiv 1 \bmod 4$, we have

$$R_{b_0 b_1}(\tau) = R_{b_1 b_0}(\tau) = \begin{cases} p-2, & \text{for } \tau = 0 \\ -1, & \text{otherwise} \end{cases}$$

and for an odd prime $p$ such that $p \equiv 3 \bmod 4$, we have

$$R_{b_0 b_1}(\tau) = \begin{cases} p-2, & \text{for } \tau = 0 \\ -1 + 2\eta(\tau), & \text{otherwise} \end{cases}$$
$$R_{b_1 b_0}(\tau) = \begin{cases} p-2, & \text{for } \tau = 0 \\ -1 - 2\eta(\tau), & \text{otherwise.} \end{cases}$$

□

## 3. New Quaternary Sequences From Legendre Sequences

Applying the inverse Gray mapping to two binary sequences in (5) and (6), we propose two construction methods of new quaternary sequences with ideal autocorrelation property.

For an odd prime $p$ such that $p \equiv 1 \bmod 4$, let $b_0(t)$ and $b_1(t)$ be binary sequences of period $p$ defined in (5) and (6), respectively. Then $b_0(t)$ has one more zero than one and $b_1(t)$ has one more one than zero in a period. Let $s_0(t)$ and $s_1(t)$ be two binary sequences of period $2p$ defined by

$$s_0(t) = \begin{cases} b_0(t), & \text{for } t \equiv 0 \bmod 2 \\ b_1(t), & \text{for } t \equiv 1 \bmod 2 \end{cases} \tag{10}$$

$$s_1(t) = \begin{cases} b_0(t), & \text{for } t \equiv 0 \bmod 2 \\ b_1(t) \oplus 1, & \text{for } t \equiv 1 \bmod 2 \end{cases} \tag{11}$$

where $\oplus$ denotes modulo 2 addition. Then we have the following lemma.

**Lemma 6:** For an odd prime $p$ such that $p \equiv 1 \bmod 4$, let $s_0(t)$ and $s_1(t)$ be binary sequences of period $2p$ defined in (10) and (11). Then the autocorrelation functions $R_{s_0}(\tau)$ and $R_{s_1}(\tau)$ of $s_0(t)$ and $s_1(t)$ are calculated as

$$R_{s_0}(\tau) = \begin{cases} 2p, & \text{for } \tau \equiv 0 \bmod 2p \\ 2(p-2), & \text{for } \tau \equiv p \bmod 2p \\ -2, & \text{otherwise} \end{cases}$$

$$R_{s_1}(\tau) = \begin{cases} 2p, & \text{for } \tau \equiv 0 \bmod 2p \\ -2(p-2), & \text{for } \tau \equiv p \bmod 2p \\ -2, & \text{for even } \tau \not\equiv 0 \bmod 2p \\ 2, & \text{for odd } \tau \not\equiv p \bmod 2p. \end{cases}$$

And their cross-correlation functions $R_{s_0 s_1}(\tau)$ and $R_{s_1 s_0}(\tau)$ are also computed as

$$R_{s_0 s_1}(\tau) = R_{s_1 s_0}(\tau) = \begin{cases} 4\eta(\tau), & \text{for even } \tau \not\equiv 0 \bmod 2p \\ 0, & \text{otherwise.} \end{cases}$$

*Proof*: From the definition of $s_0(t)$ and $s_1(t)$, we have

$$R_{s_0}(\tau) = \begin{cases} R_{b_0}(\tau) + R_{b_1}(\tau), & \text{for } \tau \equiv 0 \bmod 2 \\ 2R_{b_0 b_1}(\tau), & \text{for } \tau \equiv 1 \bmod 2 \end{cases}$$

$$R_{s_1}(\tau) = \begin{cases} R_{b_0}(\tau) + R_{b_1}(\tau), & \text{for } \tau \equiv 0 \bmod 2 \\ -2R_{b_0 b_1}(\tau), & \text{for } \tau \equiv 1 \bmod 2 \end{cases}$$

$$R_{s_0 s_1}(\tau) = R_{s_1 s_0}(\tau) = \begin{cases} R_{b_0}(\tau) - R_{b_1}(\tau), & \text{for } \tau \equiv 0 \bmod 2 \\ 0, & \text{for } \tau \equiv 1 \bmod 2. \end{cases}$$

From Lemma 5, we have

$$R_{s_0}(\tau) = \begin{cases} 2p, & \text{for } \tau \equiv 0 \bmod 2p \\ 2(p-2), & \text{for } \tau \equiv p \bmod 2p \\ -2, & \text{otherwise} \end{cases}$$

$$R_{s_1}(\tau) = \begin{cases} 2p, & \text{for } \tau \equiv 0 \bmod 2p \\ -2(p-2), & \text{for } \tau \equiv p \bmod 2p \\ -2, & \text{for even } \tau \not\equiv 0 \bmod 2p \\ 2, & \text{for odd } \tau \not\equiv p \bmod 2p \end{cases}$$

$$R_{s_0 s_1}(\tau) = R_{s_1 s_0}(\tau) = \begin{cases} 4\eta(\tau), & \text{for even } \tau \not\equiv 0 \bmod 2p \\ 0, & \text{otherwise.} \end{cases}$$

□

Applying the inverse Gray mapping to two binary sequences $s_0(t), s_1(t)$ in (10) and (11), new quaternary sequences with ideal autocorrelation property can be constructed as in the following theorem.

**Theorem 7:** For an odd prime $p$ such that $p \equiv 1 \bmod 4$, let $s_0(t)$ and $s_1(t)$ be two binary sequences defined in (10)

and (11). Let $q_1(t)$ be the quaternary sequence of period $2p$ defined by

$$q_1(t) = \phi(s_0(t), s_1(t)). \tag{12}$$

Then the autocorrelation function of $q_1(t)$ is given as

$$R_{q_1}(\tau) = \begin{cases} 2p, & \text{for } \tau \equiv 0 \bmod 2p \\ -2, & \text{for even } \tau \not\equiv 0 \bmod 2p \\ 0, & \text{for odd } \tau. \end{cases}$$

*Proof*: From Theorem 2, it is clear that $R_{q_1}(\tau)$ can be rewritten as

$$R_{q_1}(\tau) = \frac{1}{2}(R_{s_0}(\tau) + R_{s_1}(\tau)) + \frac{\omega_4}{2}(R_{s_0 s_1}(\tau) - R_{s_1 s_0}(\tau)).$$

From Lemma 6, $R_{q_1}(\tau)$ can be calculated as

$$R_{q_1}(\tau) = \begin{cases} 2p, & \text{for } \tau \equiv 0 \bmod 2p \\ -2, & \text{for even } \tau \not\equiv 0 \bmod 2p \\ 0, & \text{for odd } \tau. \end{cases}$$

□

For an odd prime $p$ such that $p \equiv 3 \bmod 4$, let $b_0(t)$ and $b_1(t)$ be two binary sequences of period $p$ in (5) and (6), respectively. And let $s_2(t)$ and $s_3(t)$ be two binary sequences of period $2p$ defined by

$$s_2(t) = \begin{cases} b_0(t), & \text{for } t \equiv 0 \bmod 2 \\ b_0(t), & \text{for } t \equiv 1 \bmod 2 \end{cases} \tag{13}$$

$$s_3(t) = \begin{cases} b_1(t), & \text{for } t \equiv 0 \bmod 2 \\ b_1(t) \oplus 1, & \text{for } t \equiv 1 \bmod 2. \end{cases} \tag{14}$$

Then we have the following lemma.

**Lemma 8:** For an odd prime $p$ such that $p \equiv 3 \mod 4$, let $s_2(t)$ and $s_3(t)$ be binary sequences of period $2p$ defined in (13) and (14). Then the autocorrelation functions $R_{s_2}(\tau)$ and $R_{s_3}(\tau)$ of $s_2(t)$ and $s_3(t)$ are calculated as

$$R_{s_2}(\tau) = \begin{cases} 2p, & \text{for } \tau \equiv 0 \bmod 2p \text{ or } \tau \equiv p \bmod 2p \\ -2, & \text{otherwise} \end{cases}$$

$$R_{s_3}(\tau) = \begin{cases} 2p, & \text{for } \tau \equiv 0 \bmod 2p \\ -2p, & \text{for } \tau \equiv p \bmod 2p \\ -2, & \text{for even } \tau \not\equiv 0 \bmod 2p \\ 2, & \text{for odd } \tau \not\equiv p \bmod 2p. \end{cases}$$

And the cross-correlation functions $R_{s_2 s_3}(\tau)$ and $R_{s_3 s_2}(\tau)$ are also calculated as

$$R_{s_2 s_3}(\tau) = R_{s_3 s_2}(\tau) = 0.$$

The proof of the above lemma is similar to that of Lemma 6 and thus we omit the proof of the above lemma.

Applying the inverse Gray mapping to two binary sequences in (13) and (14), a new quaternary sequence can be constructed as in the following theorem.

**Theorem 9:** For an odd prime $p$ such that $p \equiv 3 \bmod 4$, let $s_2(t)$ and $s_3(t)$ be binary sequences defined in (13) and (14). Let $q_2(t)$ be the quaternary sequence of period $2p$ defined by

$$q_2(t) = \phi(s_2(t), s_3(t)). \tag{15}$$

Then the autocorrelation function of $q_2(t)$ is computed as

$$R_{q_2}(\tau) = \begin{cases} 2p, & \text{for } \tau \equiv 0 \bmod 2p \\ -2, & \text{for even } \tau \not\equiv 0 \bmod 2p \\ 0, & \text{for odd } \tau. \end{cases}$$

*Proof*: From Theorem 2, it is clear that $R_{q_2}(\tau)$ can be rewritten as

$$R_{q_2}(\tau) = \frac{1}{2}(R_{s_2}(\tau) + R_{s_3}(\tau)) + \frac{\omega_4}{2}(R_{s_2 s_3}(\tau) - R_{s_3 s_2}(\tau)).$$

From Lemma 8, $R_{q_2}(\tau)$ can be calculated as

$$R_{q_2}(\tau) = \begin{cases} 2p, & \text{for } \tau \equiv 0 \bmod 2p \\ -2, & \text{for even } \tau \not\equiv 0 \bmod 2p \\ 0, & \text{for odd } \tau. \end{cases}$$

□

Using the definitions of $s_0(t)$, $s_1(t)$, $s_2(t)$, and $s_3(t)$ in (10), (11), (13), and (14), it is not difficult to derive the balance property of two proposed quaternary sequences $q_1(t)$ and $q_2(t)$ as in the following theorem.

**Theorem 10:** Let $q_1(t)$ and $q_2(t)$ be two quaternary sequences defined in Theorems 7 and 9. Then $q_1(t)$ and $q_2(t)$ have the balanced property, i.e., for $p \equiv 1 \mod 4$, we have

$$q_1(t) = \begin{cases} 0, & \frac{p+1}{2} \text{ times} \\ 1, & \frac{p-1}{2} \text{ times} \\ 2, & \frac{p-1}{2} \text{ times} \\ 3, & \frac{p+1}{2} \text{ times} \end{cases}$$

and for $p \equiv 3 \mod 4$, we have

$$q_2(t) = \begin{cases} 0, & \frac{p+1}{2} \text{ times} \\ 1, & \frac{p+1}{2} \text{ times} \\ 2, & \frac{p-1}{2} \text{ times} \\ 3, & \frac{p-1}{2} \text{ times.} \end{cases}$$

Two examples of new quaternary sequences $q_1(t)$ and $q_2(t)$ are given in the following example.

**Example 11:** For $p = 17$, two binary sequences $b_0(t), b_1(t)$ are given as

$$b_0(t) = 00010111001110100$$
$$b_1(t) = 10010111001110100.$$

Then $s_0(t)$ and $s_1(t)$ can be obtained as

$$s_0(t) = 00010111001110100100101110011101 00$$
$$s_1(t) = 01000010011011110001111011001000 01.$$

Finally, we have the quaternary sequence $q_1(t)$ given as

$$q_1(t) = 0103032301232121030121232103230301.$$

Note that the number of occurrences of each symbol of $q_1(t)$ in a period is counted as

$$q_1(t) = \begin{cases} 0, & 9 \text{ times} \\ 1, & 8 \text{ times} \\ 2, & 8 \text{ times} \\ 3, & 9 \text{ times} \end{cases}$$

and its autocorrelation distribution is computed as

$$R_{q_1}(\tau) = \begin{cases} 34, & \text{once for } \tau \equiv 0 \bmod 34 \\ -2, & 16 \text{ times for even } \tau \not\equiv 0 \bmod 34 \\ 0, & 17 \text{ times for odd } \tau. \end{cases}$$

Similarly, for $p = 19$, two binary sequences $b_0(t), b_1(t)$ are given as

$$b_0(t) = 0100111101010000110010011110101000011 0$$
$$b_1(t) = 1100111101010000110.$$

Then $s_2(t)$ and $s_3(t)$ can be obtained as

$$s_2(t) = 0100111101010000110010011110101000011 0$$
$$s_3(t) = 1001101000000101100011001010111111010011.$$

Finally, we have the quaternary sequence $q_2(t)$ given as

$$q_2(t) = 1301232303030101230021032321212101032 1.$$

Note that the number of occurrences of each symbol of $q_2(t)$ in a period is counted as

$$q_2(t) = \begin{cases} 0, & 10 \text{ times} \\ 1, & 10 \text{ times} \\ 2, & 9 \text{ times} \\ 3, & 9 \text{ times} \end{cases}$$

and its autocorrelation distribution is computed as

$$R_{q_2}(\tau) = \begin{cases} 38, & \text{once for } \tau \equiv 0 \bmod 38 \\ -2, & 18 \text{ times for even } \tau \not\equiv 0 \bmod 38 \\ 0, & 19 \text{ times for odd } \tau. \end{cases}$$

## 4. Linear Complexity of New Quaternary Sequences From Legendre Sequences

From Blahut's theorem [15], it is known that the linear complexity of a periodic sequence can be determined by counting the number of nonzero coefficients of its discrete Fourier transform.

Firstly, it seems to be natural to consider the linear complexity of a quaternary sequence over a ring $Z_4$. However, the discrete Fourier transform which is one of the main tools for the linear complexity of a sequence is defined over a field, not a ring [16]. Therefore, we need to find a proper finite field which is closely related to the quaternary sequence in Theorems 7 and 9.

In addition, since the linear complexity of a sequence is related to not only the generation of a sequence (by a legitimate user), but also the reconstruction of a sequence (by a malicious attacker), it is better to check whether there is a possible way to reconstruct the sequence or not for its security. In this respect, we will consider the linear complexity over $F_q$, where $q \geq 5$ is a prime number and not equal to $p$ and $F_{q^m}$ is the splitting field of $x^{2p} - 1$ for some integer $m$. Let $\alpha$ be a primitive $2p$-th root of unity in a finite field $F_{q^m}$ that is the splitting field of $x^{2p} - 1$.

The quaternary sequence $q_1(t)$ constructed in the previous section can be represented in terms of its component sequences as

$$q_1(t) = \phi(s_0(t), s_1(t)) = 3s_0(t) + s_1(t) - 2s_0(t)s_1(t) \tag{16}$$

using arithmetics in $F_q$. Note that this representation holds only for $q \geq 5$. The discrete Fourier coefficient is defined as

$$A_i = \frac{1}{N} \sum_{t=0}^{N-1} q(t)\alpha^{-it}$$

for $0 \leq i < 2p$. From the definition of the element $\alpha$, we have $\alpha^p = -1$ because the order of $\alpha$ is $2p$. And we have

$$\sum_{t=0}^{2p-1} \alpha^{it} = \frac{\alpha^{2pi} - 1}{\alpha^i - 1} = 0.$$

If we count the number $L_0$ of indices $i$'s satisfying $A_i = 0$, the linear complexity of $q(t)$ becomes $N - (L_0 - 1)$.

### 4.1 Derivation of the Discrete Fourier Coefficients for $p \equiv 1 \bmod 4$

From (8) and (9), we can represent intermediate sequences $s_0(t)$ and $s_1(t)$ in signal domain as

$$(-1)^{s_0(t)} = \eta(t) + I(t) - I(t-p)$$
$$(-1)^{s_1(t)} = \begin{cases} \eta(t) + I(t), & 0 \leq t < p \\ -\eta(t) + I(t-p), & p \leq t < 2p. \end{cases}$$

Therefore, we have the intermediate sequence representations as

$$s_0(t) = \frac{1}{2}[1 - \eta(t) - I(t) + I(t-p)] \tag{17}$$
$$s_1(t) = \frac{1}{2}[1 - \Xi(t) - I(t) - I(t-p)] \tag{18}$$

where

$$\Xi(t) = \begin{cases} \eta(t), & 0 \leq t < p \\ -\eta(t), & p \leq t < 2p. \end{cases}$$

Then, we can derive the discrete Fourier coefficients of the quaternary sequence $q_1(t)$ as in the following theorem.

**Theorem 12:** For $p \equiv 1 \bmod 4$, the discrete Fourier coefficients of the quaternary sequence $q_1(t)$ defined in (12) are expressed as

$$NA_{-i} = -(1+(-1)^i)\sum_{t=0}^{p-1}\eta(t)\alpha^{it} - (1-(-1)^i)\left[\frac{\alpha^i-2}{\alpha^i-1}\right].$$

*Proof*: Using (17) and (18), the discrete Fourier transform can be calculated as

$$\begin{aligned} NA_{-i} &= \sum_{t=0}^{2p-1} q_1(t)\alpha^{it} \\ &= \sum_{t=0}^{2p-1}\Big(3s_0(t)+s_1(t)-2s_0(t)s_1(t)\Big)\alpha^{it} \\ &= 3\sum_{t=0}^{2p-1} s_0(t)\alpha^{it} + \sum_{t=0}^{2p-1} s_1(t)\alpha^{it} - 2\sum_{t=0}^{2p-1} s_0(t)s_1(t)\alpha^{it}. \end{aligned} \tag{19}$$

Now, let us calculate the last three summations in (19). The first sum in (19) can be rewritten as

$$\begin{aligned} 3\sum_{t=0}^{2p-1} s_0(t)\alpha^{it} &= \frac{3}{2}\left[\sum_{t=0}^{2p-1}\alpha^{it} - \sum_{t=0}^{2p-1}\eta(t)\alpha^t - \alpha^0 + \alpha^{pi}\right] \\ &= \frac{3}{2}\left[0 - \sum_{t=0}^{p-1}\eta(t)\alpha^{it} - \sum_{t=p}^{2p-1}\eta(t)\alpha^{it} - 1 + (-1)^i\right] \\ &= -\frac{3(1+(-1)^i)}{2}\sum_{t=0}^{p-1}\eta(t)\alpha^{it} - \frac{3(1-(-1)^i)}{2}. \end{aligned}$$

The second sum in (19) can be rewritten as

$$\begin{aligned} \sum_{t=0}^{2p-1} s_1(t)\alpha^{it} &= \frac{1}{2}\left[\sum_{t=0}^{2p-1}\alpha^{it} - \sum_{t=0}^{2p-1}\eta(t)\alpha^{it} - \alpha^0 - \alpha^{pi}\right] \\ &= \frac{1}{2}\left[0 - \sum_{t=0}^{p-1}\eta(t)\alpha^{it} + \sum_{t=p}^{2p-1}\eta(t)\alpha^{it} - 1 - (-1)^i\right] \\ &= -\frac{(1-(-1)^i)}{2}\sum_{t=0}^{p-1}\eta(t)\alpha^{it} - \frac{1+(-1)^i}{2}. \end{aligned}$$

Finally, using (17) and (18), the last sum in (19) can be rewritten as

$$\begin{aligned} &2\sum_{t=0}^{2p-1} s_0(t)s_1(t)\alpha^{it} \\ &= \frac{1}{2}\sum_{t=0}^{2p-1}(1-\eta(t)-I(t)+I(t-p)) \\ &\qquad \times (1-\Xi(t)-I(t)-I(t-p))\alpha^{it} \\ &= \frac{1}{2}\sum_{t=0}^{2p-1}\Big[(1-\Xi(t)-\eta(t)+\eta(t)\Xi(t) \\ &\qquad -I(t)-I(t-p))\alpha^{it}\Big] \\ &= \frac{1}{2}\left[\sum_{t=0}^{2p-1}\alpha^{it} - \sum_{t=0}^{2p-1}\Xi(t)\alpha^{it} - \sum_{t=0}^{2p-1}\eta(t)\alpha^{it} \right. \\ &\qquad \left. + \sum_{t=0}^{2p-1}\eta(t)\Xi(t)\alpha^{it} - \alpha^0 - \alpha^{ip}\right] \\ &= \frac{1}{2}\left[0 - \sum_{t=0}^{p-1}\eta(t)\alpha^{it} + \sum_{t=p}^{2p-1}\eta(t)\alpha^{it} \right. \\ &\qquad - \sum_{t=0}^{p-1}\eta(t)\alpha^{it} - \sum_{t=p}^{2p-1}\eta(t)\alpha^{it} \\ &\qquad \left. + \sum_{t=0}^{p-1}\eta^2(t)\alpha^{it} - \sum_{t=p}^{2p-1}\eta^2(t)\alpha^{it} - 1 - (-1)^i\right] \\ &= \frac{1}{2}\left[-2\sum_{t=0}^{p-1}\eta(t)\alpha^{it} + \sum_{t=1}^{p-1}\alpha^{it} - \sum_{t=p+1}^{2p-1}\alpha^{it} - 1 - (-1)^i\right] \\ &= \frac{1}{2}\left[-2\sum_{t=0}^{p-1}\eta(t)\alpha^{it} + \sum_{t=0}^{p-1}\alpha^{it} - \sum_{t=p}^{2p-1}\alpha^{it} - 2\right] \\ &= -\sum_{t=0}^{p-1}\eta(t)\alpha^{it} - 1 + \frac{1-(-1)^i}{2}\sum_{t=0}^{p-1}\alpha^{it} \\ &= -\sum_{t=0}^{p-1}\eta(t)\alpha^{it} - 1 + \frac{1-(-1)^i}{2}\frac{\alpha^{ip}-1}{\alpha^i-1} \\ &= -\sum_{t=0}^{p-1}\eta(t)\alpha^{it} - 1 - \frac{1-(-1)^i}{\alpha^i-1}. \end{aligned}$$

Thus, we have

$$\begin{aligned} NA_{-i} &= 3\sum_{t=0}^{2p-1} s_0(t)\alpha^{it} + \sum_{t=0}^{2p-1} s_1(t)\alpha^{it} - 2\sum_{t=0}^{2p-1} s_0(t)s_1(t)\alpha^{it} \\ &= -\frac{3(1+(-1)^i)}{2}\sum_{t=0}^{p-1}\eta(t)\alpha^{it} - \frac{3(1-(-1)^i)}{2} \\ &\quad - \frac{(1-(-1)^i)}{2}\sum_{t=0}^{p-1}\eta(t)\alpha^{it} - \frac{1+(-1)^i}{2} \\ &\quad + \sum_{t=0}^{p-1}\eta(t)\alpha^{it} + 1 + \frac{1-(-1)^i}{\alpha^i-1} \\ &= -(1+(-1)^i)\sum_{t=0}^{p-1}\eta(t)\alpha^{it} - (1-(-1)^i) + \frac{1-(-1)^i}{\alpha^i-1}. \end{aligned}$$

□

### 4.2 Derivation of the Discrete Fourier Coefficients for $p \equiv 3 \bmod 4$

Now, for $p \equiv 3 \bmod 4$, we will consider the linear complexity of the quaternary sequence given in Theorem 9. Firstly, we have the intermediate sequence representation as

$$s_2(t) = \frac{1}{2}[1 - \eta(t) - I(t) - I(t-p)] \tag{20}$$

$$s_3(t) = \frac{1}{2}[1 - \Xi(t) + I(t) - I(t-p)] \tag{21}$$

where

$$\Xi(t) = \begin{cases} \eta(t), & 0 \le t < p \\ -\eta(t), & p \le t < 2p. \end{cases}$$

Then, the discrete Fourier transform of $q_2(t)$ is given as follows.

**Theorem 13:** For $p \equiv 3 \bmod 4$, the discrete Fourier coefficients of the quaternary sequence $q_1(t)$ defined in (12) are given as

$$NA_{-i} = -(1 + (-1)^i) \sum_{t=0}^{p-1} \eta(t)\alpha^{it} - 2(-1)^i + \frac{1-(-1)^i}{\alpha^i - 1}.$$

*Proof*: Using (20) and (21), the discrete Fourier transform can be similarly calculated as

$$NA_{-i} = 3\sum_{t=0}^{2p-1} s_2(t)\alpha^{it} + \sum_{t=0}^{2p-1} s_3(t)\alpha^{it} - 2\sum_{t=0}^{2p-1} s_2(t)s_3(t)\alpha^{it}. \tag{22}$$

Not, let us calculate the last three summations in (19). The first sum in (19) can be rewritten as

$$3\sum_{t=0}^{2p-1} s_2(t)\alpha^{it} = -\frac{3(1+(-1)^i)}{2}\sum_{t=0}^{p-1}\eta(t)\alpha^{it} - \frac{3(1+(-1)^i)}{2}.$$

The second sum in (19) can be rewritten as

$$\sum_{t=0}^{2p-1} s_3(t)\alpha^{it} = -\frac{(1-(-1)^i)}{2}\sum_{t=0}^{p-1}\eta(t)\alpha^{it} + \frac{1-(-1)^i}{2}.$$

Finally, using (20) and (21), the last sum in (19) can be rewritten as

$$\begin{aligned} 2\sum_{t=0}^{2p-1} s_2(t)s_3(t)\alpha^{it} &= \frac{1}{2}\sum_{t=0}^{2p-1}\Big[(1 - \Xi(t) - \eta(t) + \eta(t)\Xi(t) \\ &\qquad - I(t) - I(t-p))\alpha^{it}\Big] \\ &= -\sum_{t=0}^{p-1}\eta(t)\alpha^{it} - 1 - \frac{1-(-1)^i}{\alpha^i - 1}. \end{aligned}$$

Thus, we have

$$\begin{aligned} NA_{-i} &= 3\sum_{t=0}^{2p-1} s_2(t)\alpha^{it} + \sum_{t=0}^{2p-1} s_3(t)\alpha^{it} - 2\sum_{t=0}^{2p-1} s_2(t)s_3(t)\alpha^{it} \\ &= -\frac{3(1+(-1)^i)}{2}\sum_{t=0}^{p-1}\eta(t)\alpha^{it} - \frac{3(1+(-1)^i)}{2} \\ &\quad - \frac{(1-(-1)^i)}{2}\sum_{t=0}^{p-1}\eta(t)\alpha^{it} + \frac{1-(-1)^i}{2} \\ &\quad + \sum_{t=0}^{p-1}\eta(t)\alpha^{it} + 1 + \frac{1-(-1)^i}{\alpha^i - 1} \\ &= -(1+(-1)^i)\sum_{t=0}^{p-1}\eta(t)\alpha^{it} - 2(-1)^i + \frac{1-(-1)^i}{\alpha^i - 1}. \end{aligned}$$

□

### 4.3 Linear Complexity over the Splitting Field $F_{q^m}$ ($m > 1$)

In this subsection, we will derive the linear complexity of quaternary sequences over the splitting field $F_{q^m}$. Firstly, let us consider the case of odd $i$. From Theorem 12, the number of odd $i$'s satisfying $A_{-i} = 0$ for $p \equiv 1 \bmod 4$ can be counted by finding $i$ such as

$$NA_{-i} = -2\left[\frac{\alpha^i - 2}{\alpha^i - 1}\right] = 0 \tag{23}$$

namely, $\alpha^i = 2$. Since the order of $\alpha$ is $2p$ and $\gcd(i, 2p) = 1$ for $\alpha^i = 2$, the order of the element 2 is also $2p$. This means that $2^{2p} \equiv 1 \bmod q$ or equivalently, $q \mid (2^p + 1)$.

Similarly, from Theorem 13, the number of odd $i$'s satisfying $A_{-i} = 0$ for $p \equiv 3 \bmod 4$ can be counted by finding $i$ such as

$$NA_{-i} = 2 + \frac{2}{\alpha^i - 1} = 0 \tag{24}$$

which means that $\alpha^i = 0$, a contradiction since $\alpha$ has nonzero order.

From (23) and (24), we have

$$|\{i \mid A_{-i} = 0, i \equiv 1 \bmod 2\}| = \begin{cases} 1, & \text{if } p \equiv 1 \bmod 4 \\ 0, & \text{if } p \equiv 3 \bmod 4 \end{cases}$$

Let $\beta$ be a primitive element of $F_{q^m}$ ($m > 1$). Then, we have $\alpha = \beta^{\frac{q^m-1}{2p}}$. It is clear that $\alpha^i$ ($0 \le i < 2p$) is in $F_q$ if and only if $2p \mid (q-1)$. Therefore, we can summarize the discussion as in the following proposition

**Proposition 14:** For odd $i$, the number of $i$'s satisfying $A_{-i} = 0$ is 1 if the element 2 is a quadratic non-residue in $F_q$, $2p \mid (q-1)$, and $q \mid (2^p + 1)$ for $p \equiv 1 \bmod 4$. Otherwise, the number is zero.

Now, let us consider the case of even $i$. From Theorems 12 and 13, for even $i$ and $p \equiv 1 \bmod 4$, the discrete Fourier coefficient can be presented as

$$NA_{-i} = -2\sum_{t=0}^{p-1}\eta(t)\alpha^{it} \tag{25}$$

or if $p \equiv 3 \bmod 4$,

$$NA_{-i} = -2\sum_{t=0}^{p-1}\eta(t)\alpha^{it} - 2. \tag{26}$$

Note that in (25) and (26), $\sum_{t=0}^{p-1}\eta(t)\alpha^{it}$ can be rewritten as

$$\sum_{t=0}^{p-1}\eta(t)\alpha^{it}=\sum_{t\in QR\setminus\{0\}}\alpha^{it}-\sum_{t\in QNR}\alpha^{it}$$

where $QR$ and $QNR$ are the sets of quadratic residues and quadratic non-residues of $F_p$, respectively. If $\alpha^i\neq 1$, we have

$$\begin{aligned}\sum_{t\in QR\setminus\{0\}}\alpha^{it}+\sum_{t\in QNR}\alpha^{it}&=\sum_{t=1}^{p-1}\alpha^{it}=\sum_{t=0}^{p-1}\alpha^{it}-1\\&=\frac{\alpha^{ip}-1}{\alpha^i-1}-1\equiv q-1 \bmod q.\end{aligned}\tag{27}$$

The last congruence holds because $\alpha^{ip}=1$ for even $i$. If $\alpha^i=1$ (i.e, $i\equiv 0 \bmod 2p$), we have

$$\sum_{t\in QR\setminus\{0\}}\alpha^{it}+\sum_{t\in QNR}\alpha^{it}=\sum_{t=0}^{p-1}\alpha^{it}-1=p-1 \bmod q.\tag{28}$$

Therefore, from (27) and (28), we have

$$NA_{-i}=\begin{cases}-4S(\alpha^i)+2p-2, & \text{if } i\equiv 0 \bmod 2p\\ -4S(\alpha^i)-2, & \text{otherwise}\end{cases}\tag{29}$$

for $p\equiv 1 \bmod 4$ and

$$NA_{-i}=\begin{cases}-4S(\alpha^i)+2p-4, & \text{if } i\equiv 0 \bmod 2p\\ -4S(\alpha^i)-4, & \text{otherwise}\end{cases}\tag{30}$$

for $p\equiv 3 \bmod 4$ where $S(\alpha^i)=\sum_{t\in QR\setminus\{0\}}\alpha^{it}$. Thus, the number of even $i$'s satisfying $A_{-i}=0$ can be counted by evaluating the sum $S(\alpha^i)$ for even $i$, $0\le i<2p$. For this purpose, we need the following lemma.

**Lemma 15:** We have the following basic facts:

1) $uQR=QR$ for any quadratic residue $u$ in $F_p$
2) $uQR=QNR$ for any quadratic non-residue $u$ in $F_p$.

The values of $S(\alpha^i)$ can be evaluated according to two cases, $q\in QR$ or $q\in QNR$.

**Lemma 16:** For even $i$, $S(\alpha^i)$ is in the prime field $F_q$ if and only if $q$ is a quadratic residue of $F_p$ or $q^m$ is a prime (i.e., $m=1$).

*Proof*: Note that we have $[S(\alpha^i)]^q=S(\alpha^{iq})$ because the characteristic of $F_{q^m}$ is $q$. If $q\in QR$, from 1) of Lemma 15, we have $[S(\alpha^i)]^q=S(\alpha^i)$. □

Note that if $i=0$, we have $S(1)=(p-1)/2$. From (29), we have $A_0\equiv 0 \bmod q$ for $p\equiv 1 \bmod 4$. However, from (30), $A_0\not\equiv 0 \bmod q$ for $p\equiv 3 \bmod 4$.

For even $i\neq 0$ and $p\equiv 1 \bmod 4$, from (29), if $S(\alpha^i)=(q-1)/2 \bmod q$, we have $A_{-i}\equiv 0 \bmod q$. Since the values of $S(\alpha^i)$ are the same for all elements in $QR$ or $QNR$, respectively, the number of such $i$'s is $(p-1)/2$. From $S(\alpha^{t_Q})+S(\alpha^{t_N})=q-1$ for even $i$, we have $S(\alpha^{t_Q})=S(\alpha^{t_N})=(q-1)/2$, where $t_Q\in QR$ and $t_N\in QNR$. Therefore, the number of even $i$'s is $p-1$, when $S(\alpha^{t_Q})=(q-1)/2$.

Similarly, for even $i\neq 0$ and $p\equiv 3 \bmod 4$, from (30), $A_{-i}\equiv 0 \bmod q$ if $S(\alpha^i)=q-1$. Thus, the number of even $i$'s is $(p-1)/2$, when $S(\alpha^{t_Q})=q-1$ or $S(\alpha^{t_N})=0$. We can summarize these results as in the following theorem.

**Theorem 17:** For $p\equiv 1 \bmod 4$, the linear complexity over $F_q$ of the quaternary sequence $q_1(t)$ defined in (12) is given as if $S(\alpha^{t_Q})=S(\alpha^{t_N})=(q-1)/2$, where $t_Q\in QR$ and $t_N\in QNR$,

$$L_0=\begin{cases}p-1, & \text{if 2 is a QNR in } F_q, 2p|(q-1),\\ & \quad\text{and } q|(2^p+1)\\ p, & \text{otherwise}\end{cases}$$

and otherwise

$$L_0=\begin{cases}2p-2, & \text{if 2 is a QNR in } F_q, 2p|(q-1),\\ & \quad\text{and } q|(2^p+1)\\ 2p-1, & \text{otherwise.}\end{cases}$$

Similarly, the linear complexity of the quaternary sequence $q_2(t)$ is given as in the following theorem.

**Theorem 18:** For $p\equiv 3 \bmod 4$, the linear complexity over $F_q$ of the quaternary sequence $q_2(t)$ defined in (15) is given as

$$L_0=\begin{cases}(3p+1)/2, & \text{if } S(\alpha^{t_Q})=q-1\\ 2p, & \text{otherwise}\end{cases}$$

where $t_Q\in QR$ and $t_N\in QNR$.

### 4.4 Linear Complexity over the Splitting Field $F_q$

In this subsection, let us consider the case of $m=1$ as a special case of the previous results. Then, we have a prime $q=2p+1$ for a prime $p$ and $\alpha$ is in $F_q$. In this case, the prime $p$ is called as a Sophie Germain prime whose elements can be listed as $\{5, 11, 23, 29, 41, 53, 83, 89, 113, 131, 173, 179, 191, 233, \cdots\}$ for $q\ge 5$.

**Lemma 19:** Let $q=2p+1$ be a prime where $p$ is a prime. Then, we have

$$2 \text{ is } \begin{cases}\text{a quadratic resiue of } F_q, & \text{if } p\equiv 1 \bmod 4\\ \text{a quadratic non-resiude of } F_q, & \text{if } p\equiv 3 \bmod 4.\end{cases}$$

*Proof*: Firstly, consider the case of $p\equiv 1 \bmod 4$. Then $p$ can be represented as $p=8k+1$ or $p=8k+5$ for some $k$. Thus, we have $q=2p+1\equiv 3 \bmod 8$. Conversely, for the case of $p\equiv 3 \bmod 4$, we have $q=2p+1\equiv 7 \bmod 8$. From the property of Legendre symbol, 2 is a square in $F_q$ if and only if $(-1)^{(q^2-1)/8}=1$. Therefore, we prove this lemma. □

For odd $i$, the number of $i$'s satisfying (23) is 1 if 2 is a quadratic non-residue in $F_q$. From Lemma 19, for $p\equiv$

1 mod 4, the number of $i$'s satisfying (23) is zero.

Therefore, in Theorem 17, for $p \equiv 1 \bmod 4$, 2 is always a quadratic residue of $F_q$. Then Theorem 17 can be simplified as in the following corollary.

**Corollary 20:** For $p \equiv 1 \bmod 4$ and $q = 2p + 1$, the linear complexity over $F_q$ of the quaternary sequence $q_1(t)$ defined in (12) is given as

$$L_0 = \begin{cases} p, & \text{if } S(\alpha^{t_Q}) = S(\alpha^{t_N}) = (q-1)/2 \\ 2p-1, & \text{otherwise.} \end{cases}$$

### 4.5 Examples

In this subsection, we present some examples to clearly demonstrate the results of this paper.

**Example 21:** Let $p = 5 \equiv 1 \bmod 4$. We have a quaternary sequence $q_2(t)$ with period 10 from the Legendre sequence with period 5. Suppose that a splitting field of $x^{10} - 1$ is chosen as $F_{11}$, where $q = 11$ and $m = 1$. It is obvious that $S(\alpha^{t_Q})$ is always in $F_{11}$. Let $\alpha = 2$ be a primitive element of the finite field $F_{11}$ and a primitive $2p$-th root of unity, at the same time. The set of quadratic residues $QR$ of $F_5$ can be obtained as $\{0, 1, 4\}$. Then for even $i \in QR$, we have $S(\alpha^{t_Q}) = \alpha^4 + \alpha^6 = 3 \in F_{11}$. Therefore, we have $S(\alpha^{t_N}) = 7$. From Corollary 20, the linear complexity of the quaternary sequence is given as 9.

**Example 22:** Let $p = 11 \equiv 3 \bmod 4$. Then, we have a quaternary sequence $q_2(t)$ with period 22 from the Legendre sequence with period 11. Suppose that a splitting field of $x^{22} - 1$ is chosen as $F_{5^5}$, where $q = 5$ and $m = 5$. Let $\beta$ be a primitive element of $F_{5^5}$. Then a primitive $2p$-th root of unity can be found as $\alpha = \beta^{142}$ whose order is 22. The set of quadratic residues $QR$ of $F_{11}$ can be obtained as $\{0, 1, 3, 4, 5, 9\}$. Then for even $i \in QR$, we have $S(\alpha^{t_Q}) = \alpha^{568} + \alpha^{1704} + \alpha^{1988} + \alpha^{2272} + \alpha^{2840} = 2 \in F_5$. Therefore, we have $S(\alpha^{t_N}) = 2$ from (28). From Theorem 18, the linear complexity of the quaternary sequence is given as 22.

**Example 23:** Let $p = 19 \equiv 3 \bmod 4$. Then, we can obtain a quaternary sequence $q_2(t)$ with period 38 from the Legendre sequence with period 19. Suppose that a splitting field of $x^{38} - 1$ is chosen as $F_{7^3}$, where $q = 7$ and $m = 3$. Let $\beta$ be a primitive element of the finite field $F_{7^3}$. Then a primitive $2p$-th root of unity is found as $\alpha = \beta^9$ whose order is 38. The set of quadratic residues $QR$ of $F_{19}$ can be obtained as $\{0, 1, 4, 5, 6, 7, 9, 11, 16, 17\}$. Then, for even $i \in QR$, we have $S(\alpha^{t_Q}) = \alpha^4 + \alpha^6 + \alpha^{16} + \alpha^{20} + \alpha^{24} + \alpha^{26} + \alpha^{28} + \alpha^{30} + \alpha^{36} = 5 \in F_7$. Therefore, we have $S(\alpha^{t_N}) = 1$. From Theorem 18, the linear complexity of the quaternary sequence is given as 38, which is the same as its period. This means that there is no shorter way to represent the quaternary sequence of period 38 rather than using itself over the finite field $F_{7^3}$.

**Example 24:** Let $p = 31 \equiv 3 \bmod 4$. Then, we can obtain a quaternary sequence $q_2(t)$ with period 62 from the Legendre sequence with period 31. Suppose that a splitting field of $x^{62} - 1$ is chosen as $F_{5^3}$, where $q = 5$ and $m = 3$. Let $\beta$ be a primitive element of the finite field $F_{5^3}$. Then a primitive $2p$-th root of unity is found as $\alpha = \beta^2$ whose order is 62. The set of quadratic residues $QR$ of $F_{31}$ can be obtained as $\{0, 1, 2, 4, 5, 7, 8, 9, 10, 14, 16, 18, 19, 20, 25, 28\}$. Then for even $i \in QR$, we have $S(\alpha^{t_Q}) = \alpha^2 + \alpha^4 + \alpha^8 + \alpha^{10} + \alpha^{14} + \alpha^{16} + \alpha^{18} + \alpha^{20} + \alpha^{28} + \alpha^{32} + \alpha^{36} + \alpha^{38} + \alpha^{40} + \alpha^{50} + \alpha^{56} = 2 \in F_5$. Therefore, we have $S(\alpha^{t_N}) = 2$. From Theorem 18, the linear complexity of the quaternary sequence is given as 62, which is the same as its period. This means that there is no shorter way to represent the quaternary sequence of period 62 rather than using itself over the finite field $F_{5^3}$.

As in these examples, the linear complexities of the quaternary sequences defined in Sect. 3 are $2p - 1$ or $2p$, which are almost the same as their period $2p$ in the most cases. Only when the sum $S(\alpha^i)$ can meet a specific value for a given finite field, the linear complexity can be half of the period of the sequences.

## 5. Conclusion

In this paper, we construct new quaternary sequences of even period $2p$ using the binary Legendre sequences of period $p$ of an odd prime. For the new sequences, we derive the autocorrelation distribution, where the autocorrelation is optimal not only for $p \equiv 3 \bmod 4$, but also for $p \equiv 1 \bmod 4$. Considering the fact that the autocorrelation values of the binary Legendre sequences are optimal only when $p \equiv 3 \bmod 4$, the proposed sequences are an interesting result.

And we also derive the linear complexity of the proposed sequences by counting non-zero coefficients of the discrete Fourier transform over the finite field $F_q$, which is the splitting field of $x^{2p} - 1$. Here, if we carefully choose the related parameters such as $p$, $q$, and $m$, we can obtain the sequence with the largest linear complexity.

## Acknowledgments

This work was supported by the National Research Foundation of Korea (NRF) grants funded by the Korea government (MEST) (No. 2011-0016664).

### References

[1] H. Dieter Luke, H.D. Schotten, and H. Hadinejad-Mahram, "Binary and quadriphase sequences with optimal autocorrelation properties: A Survey," IEEE Trans. Inf. Theory, vol.49, no.12, pp.3271–3282, Dec. 2003.

[2] J.F. Dillon and H. Dobbertin, "New cyclic difference sets with Singer parameters," Finite Fields Appl., vol.10, no.3, pp.342–389, July 2004.

[3] B. Gordon, W.H. Mills, and L.R. Welch, "Some new difference sets," Canadian J. Math., vol.14, no.4, pp.614–625, 1962.

[4] J.-S. No, H. Chung, and M.S. Yun, "Binary pseudorandom sequences of period $2^n - 1$ with ideal autocorrelation generated by the polynomial $z^d + (z + 1)^d$," IEEE Trans. Inf. Theory, vol.44, no.3, pp.1278–1282, May 1998.

[5] Y.-S. Kim, J.-S. Chung, J.-S. No, and H. Chung, "On the autocorrelation distributions of Sidel'nikov sequences," IEEE Trans. Inf. Theory, vol.51, no.9, pp.3303–3307, Sept. 2005.
[6] V.M. Sidel'nikov, "Some $k$-valued pseudo-random sequences and nearly equidistant codes," Probl. Inf. Transm., vol.5, no.1, pp.12–16, 1969.
[7] H.D. Schotten, "New optimum ternary complementary sets and almost quadriphase, perfect sequences," Proc. Int. Conf. Neural Networks and Signal Process.'95, pp.1106–1109, Nanjing, China, Dec. 1995.
[8] H.D. Schotten, "Optimum complementary sets and quadriphase sequences derived from $q$-ary $m$-sequences," Proc. IEEE Int. Symp. Inf. Theory'97, p.485, Ulm, Germany, 1997.
[9] S.M. Krone and D.V. Sarwate, "Quadriphase sequences for spread spectrum multiple-access communication," IEEE Trans. Inf. Theory, vol.IT-30, no.3, pp.520–529, May 1984.
[10] C.E. Lee, "Perfect $q$-ary sequences from multiplicative characters over $GF(p)$," Electron. Lett., vol.28, pp.833–835, 1992.
[11] J.-W. Jang, Y.-S. Kim, S.-H. Kim, and J.-S. No, "New quaternary sequences with ideal autocorrelation constructed from binary sequences with ideal autocorrelation," Proc. 2009 IEEE Int. Symp. Inf. Theory (Seoul, Korea), pp.278–281, June-July 2009.
[12] Y.-S. Kim, J.-W. Jang, S.-H. Kim, and J.-S. No, "New construction of quaternary sequences with ideal autocorrelation from Legendre sequences," Proc. 2009 IEEE Int. Symp. Inf. Theory, pp.282–285, Seoul, Korea, June-July 2009.
[13] Y.-S. Kim, J.-W. Jang, S.-H. Kim, and J.-S. No, "Linear Complexity of Quaternary Sequences from Binary Legendre Sequences," Proc. ISITA 2012, pp.611–614, Hawaii, USA, Oct. 2012.
[14] T. Storer, Cyclotomy and Difference Sets, Lectures in Advanced Mathematics, Markham, Chicago, IL, 1967.
[15] R.E. Blahut, "Transform techniques for error control codes," IBM J. Res. Develop., vol.23, pp.299–315, 1979.
[16] J.L. Massey, "The discrete Fourier transform in coding and cryptography," Proc. ITW'98, San Diego, CA, Feb. 1998.
[17] C. Ding, T. Helleseth, and W. Shan, "On the linear complexity of Legnedre sequences," IEEE Trans. Inf. Theory, vol.44, no.3, pp.1276–1279, May 1998.
[18] J.-H. Kim and H.-Y. Song, "Trace representation of Legendre sequences," Des. Codes Cryptogr., vol.24, no.3, pp.343–348, 2001.
[19] H. Aly and A. Winterhof, "On the $k$-error linear complexity over $F_p$ of Legendre and Sidelnikov sequences," Des. Codes Cryptogr., vol.40, no.3, pp.369–374, 2006.
[20] Y.-S. Kim, J.-W. Jang, S.-H. Kim, and J.-S. No, "New quaternary sequences with optimal autocorrelation," Proc. IEEE ISIT 09, pp.286–289.
[21] X. Tang and C. Ding, "New classes of balanced quaternary and almost balanced binary sequences with optimal autocorrelation value," IEEE Trans. Inf. Theory, vol.56, no.12, pp.6398–6405, 2010.
[22] T. Lim, J.-S. No, and H. Chung, "New construction of quaternary sequences with good correlation using binary sequences with good correlation," IEICE Trans. Fundamentals, vol.E94-A, no.8, pp.1701–1705, Aug. 2011.
[23] Z. Yang and P. Ke, "Construction of quaternary sequences of length pq with low autocorrelation," Cryptography and Communications, vol.3, no.2, pp.55–64, 2011.
[24] J.-H. Chung, Y.-K. Han, and K. Yang, "New quaternary sequenes with even period and three-valued autocorrelation," IEICE Trans. Fundamentals, vol.E93-A, no.1, pp.309–315, Jan. 2010.
[25] F. Zeng, X. Zeng, Z. Zhang, and G. Xuan, "Optimal quaternary sequences derived from optimal binary sequences with odd length," Proc. Signal Design and its Applications in Communications (IWSDA), 2011 Fifth International Workshop, pp.80–83, 2011.
[26] J.-W. Jang and S.-H. Kim, "Quaternary sequences with good autocorrelation constructed by Gray mapping," IEICE Trans. Fundamentals, vol.E92-A, no.8, pp.2139–2140, Aug. 2009.

**Young-Sik Kim** received B.S., M.S., and Ph.D. degrees in electrical engineering and computer science from Seoul National University in 2001, 2003, and 2007, respectively. He joined Semiconductor Division, Samsung Electronics and carried out research and development for secure hardware IPs for various embedded systems, especially for smartcards until the end of August in 2010. He is an assistant professor at Chosun University, Gwangju, Korea. His research interests include cryptographic engineering and information theory including hardware security, embedded security, physical layer security, data hiding, channel coding, and signal design.

**Ji-Woong Jang** was born in 1976. He received the B.S., M.S., and Ph.D. degrees in Electrical Engineering and Computer Science from Seoul National University, Seoul, Korea, in 2000, 2002, and 2006, respectively. After Ph.D., he was a Senior Engineer at Samsung Electronics until June 2008. He was a postdoc. at UCSD from Aug. 2008 to July 2009. From Sept. 2009, he was a Senior Engineer at LG Electronics until Aug. 2012. He joined the Department of Computer and Information Technology, Ulsan College, Ulsan, Korea where he serves currently as an Assistant Professor. His research interests includes pseudo-noise (PN) sequences, difference sets, cryptography, error correcting codes, cooperative communications and wireless communication systems.

**Sang-Hyo Kim** received his B.S., M.S., and Ph.D. degrees in Electrical Engineering from Seoul National University, Seoul, Korea in 1998, 2000, and 2004, respectively. From 2004 to 2006, he was a senior engineer at Samsung Electronics. He visited University of Southern California as a visiting scholar from 2006 to 2007. In 2007, He joined the School of Information and Communication Engineering, Sungkyunkwan University, Suwon, Korea where he serves currently as an Associate Professor. His research interests include error correcting codes, pseudo random sequences, cooperative communications, distributed source coding, etc.

**Jong-Seon No** received the B.S. and M.S.E.E. degrees in electronics engineering from Seoul National University, Seoul, Korea, in 1981 and 1984, respectively, and the Ph.D. degree in electrical engineering from the University of Southern California, Los Angeles, in 1988. He was a Senior MTS at Hughes Network Systems from February 1988 to July 1990. He was also an Associate Professor in the Department of Electronic Engineering, Konkuk University, Seoul, Korea, from September 1990 to July 1999. He joined the faculty of the Department of Electrical Engineering and Computer Science, Seoul National University, in August 1999, where he is currently a Professor. His research interests include error-correcting codes, sequences, cryptography, space-time codes, LDPC codes, and wireless communication systems.