About the linear complexity of sequences over the finite field obtained by inverse Gray mapping from binary sequences

Vladimir Edemskiy, Andrey Ivanov

***Abstract*—We consider the sequences over the finite field of four elements obtained by inverse Gray mapping from a pair of binary sequences. We derive the linear complexity and the minimal polynomial of sequences constructed from Legendre sequences, Hall's sextic sequences and twin-prime sequences using the technique proposed by Tang, Ding, Lim, Kim et al.**

***Index Terms*—Binary sequences, Gray map, linear complexity, finite field**

I. Introduction

The autocorrelation is a measure of pseudo-random sequence significant for their application in wireless communications, cryptography and radar applications and so on [3], [9]. In such applications, the absolute value of the out-of-phase autocorrelation of a pseudo-random sequence is expected to be as small as possible. The linear complexity is another important parameter of pseudo-random sequence for cryptographic applications [3] (one more approach see in [1], [2]).

Tang, Ding, Lim, Kim et al. constructed new balanced quaternary sequences with optimal autocorrelation values [12], [16], [17] using the interval structure and the inverse Gray map. In the same way, we can build the sequences over the finite field of four elements from a pair of binary sequences.

In this paper we investigate the linear complexity of above mentioned sequences over the finite field of four elements. We derive the linear complexity and the minimal polynomial of sequences constructed from Legendre sequences, Hall's sextic sequences and twin-prime sequences. Binary Legendre sequences or Hall's sextic sequences and twin-prime sequences are well-known classes of sequences with a good autocorrelation function. For the application of sequences over the finite field, see [14], for instance.

II. Preliminaries

Let $c = c_0, \dots, c_{M-1}$ and $d = d_0, \dots, d_{M-1}$ be binary sequences of period M. The well-known Gray mapping $\phi : \mathbb{Z}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2$ is defined as

$$\phi(0) = (0,0),\ \phi(1) = (0,1),\ \phi(2) = (1,1),\ \phi(3) = (1,0).$$

Let $\mathbb{F}_4 = \{0, 1, \mu, \mu+1\}$ be a finite field of four elements. If we view $\mathbb{F}_4$ as a vector space over $\mathbb{F}_2$ with the basis $\mu,\ 1$, then we can define a sequence v by inverse Gray map as

$$v_i = \begin{cases} 0, & \text{if } (c_i, d_i) = (0,0), \\ 1, & \text{if } (c_i, d_i) = (0,1), \\ \mu+1, & \text{if } (c_i, d_i) = (1,1), \\ \mu, & \text{if } (c_i, d_i) = (1,0). \end{cases} \tag{1}$$

So, we can obtain a sequence over the finite field of four elements from a pair of binary sequences by the inverse Gray mapping. Next, we will use the notation $v = [c, d]$ for the sequence v obtained from a pair of sequences c, d by (1).

The linear complexity (or rank) of a sequence v over the finite field $\mathbb{F}_4$ is defined to be the smallest positive integer LC for which there exist constants $c_1, ..., c_{LC}, c_i \in \mathbb{F}_4$ such that

$$-v_m = c_1 v_{m-1} + c_2 v_{m-2} + \cdots + c_{LC} v_{m-LC} \text{ for all } m \geq LC.$$

The polynomial $m(x) = x^{LC} + c_1 x^{LC-1} + \cdots + c_{LC}$ is called the minimal polynomial of v. The linear complexity also may be defined as the length of the shortest linear feedback shift register that is capable of generating the sequence. Knowledge of just $2LC$ consecutive digits of the sequence is sufficient to enable the remainder of the sequence to be constructed. Thus, it is reasonable to suggest that 'good' sequences have the linear complexity greater than a half of a period $LC > M/2$ (where M denotes the period of the sequence) [3].

The minimal polynomial $m(x)$ and the linear complexity LC of v are given by the following equations [3]:

$$m(x) = (x^M - 1)/\gcd\big(x^M - 1, s_v(x)\big),$$
$$LC = M - \deg \gcd\big(x^M - 1, s_v(x)\big), \tag{2}$$

where $s_v(x)$ is the generating polynomial of v. Thus, $s_v\,(x) = \sum_{i=0}^{M-1} v_i x^i$. So, we must define the greatest common divisor of two polynomials.

Lemma 1: [8] Let v be defined by (1), i.e. $v = [c, d]$. Then

$$s_v(x) = \mu s_c(x) + s_d(x),$$

where $s_c\,(x) = \sum_{i=0}^{M-1} c_i x^i$ and $s_d\,(x) = \sum_{i=0}^{M-1} d_i x^i$. We see that the statement of Lemma 1 follows from (1).

In conclusion of the section we consider a simple example of using Lemma 1.

Example. Let $M = p$ where p is a prime, $p \equiv 3 (\bmod\ 4)$. Well-known Legendre sequences are defined as

$$l_j = \begin{cases} 0, & \text{if } j \bmod p = 0, \\ \left(\frac{j}{p}\right), & \text{if } j \bmod p \neq 0, \end{cases}$$

V. Edemskiy is with the Department of Applied Mathematics and Information Science, Novgorod State University, Veliky Novgorod, Russia, 173003 e-mail: Vladimir.Edemsky@novsu.ru.

A. Ivanov is with Novgorod State University, e-mail: dk@live.ru.

This work was supported by the Ministry of Education and Science of Russia as a part of state-sponsored project

where $\left(\frac{j}{p}\right)$ is Legendre symbol. Here and hereafter $a \bmod\ p$ denotes the least nonnegative integer that is congruent to a modulo p.

Let $\mathbf{QR}_p$ and $\mathbf{NQR}_p$ denote all the nonzero squares and non-squares in $\mathbb{Z}_p$, respectively. Let α be a primitive p-th root of unity in the extension of the field $\mathbb{F}_4$ ($\alpha = \mu$ for $p = 3$). It is known to exist by Galois theory. Then, by (2) and by Lemma 1, to compute the minimal polynomial and the linear complexity of v it is sufficient to know the values of polynomial $s_l(x)$ in the set $\{\alpha^j, j = 0, 1, \dots, p-1\}$.

The linear complexity of Legendre sequences was studied in [4]. In particular, it was shown that with an appropriate choice of α we can assume that

$$s_l(\alpha^j) = \begin{cases} 1, & \text{if } j \in \mathbf{QR}_p, \\ 0, & \text{if } j \in \mathbf{NQR}_p \end{cases} \tag{3}$$

for $p \equiv 7 (\bmod\ 8)$, and

$$s_l(\alpha^j) = \begin{cases} \mu, & \text{if } j \in \mathbf{QR}_p, \\ \mu + 1, & \text{if } j \in \mathbf{NQR}_p \end{cases} \tag{4}$$

for $p \equiv 3 (\bmod\ 8)$.

Let $v = [l, L^m l]$. Here L denotes the left cyclic shift operator, m is a integer, $0 < m < p$. In this case, we have that $s_{L^m l}(x) = x^{p-m} s_l(x)$ [18]. Then, by Lemma 1 we obtain the following relation

$$s_v(\alpha^j) = \mu s_l(\alpha^j) + \alpha^{-mj} s_l(\alpha^j).$$

Hence, by (3) and (4), $s_v(\alpha^j) = 0, j = 0, 1, \dots, p-1$ iff $j \in \mathbf{NQR}_p$ and $p \equiv 7 (\bmod\ 8)$. So, if $v = [l, L^m l]$ then

$$LC = \begin{cases} (p+1)/2, & \text{if } p \equiv 7 (\bmod\ 8), \\ p, & \text{if } p \equiv 3 (\bmod\ 8). \end{cases}$$

In the following sections we investigate the linear complexity and the minimal polynomial of sequences constructed by (1) using the technique proposed by Tang, Ding, Lim, Kim et al.

III. The linear complexity of Tang and Ding sequences

First of all, we consider the design of sequences proposed by Tang and Ding. Let $a = a_0, \dots, a_{N-1}$ and $b = b_0, \dots, b_{N-1}$ be binary sequences of period N, $N \equiv 3 (\bmod 4)$. In this case define sequences c and d as

$$c_i = \begin{cases} a_{i/2}, & \text{if } i \equiv 0 (\bmod 2), \\ a_{(i+N)/2}, & \text{if } i \equiv 1 (\bmod 2). \end{cases}$$

$$d_i = \begin{cases} b_{i/2}, & \text{if } i \equiv 0 (\bmod 2), \\ b_{(i+N)/2} + 1, & \text{if } i \equiv 1 (\bmod 2), \end{cases} \tag{5}$$

i.e. $c = I(a, L^{1/2} a)$ and $d = I(b, L^{1/2} b + 1)$, where I denotes the interleaved operator [17].

In their paper [17], Tang and Ding proved that a sequence $u : u_i = \phi^{-1}(c_i, d_i)$ is balanced quaternary sequence with optimal autocorrelation values if a, b are binary sequences with optimal autocorrelation value.

Here we investigate the linear complexity of sequences constructed by (1) when a, b are Legendre sequences, Hall's sextic sequences and twin-prime sequences. The results of this section were presented at the conference [7].

By definition of c, d we have that $M = 2N$ and by (2) we obtain

$$m(x) = (x^N - 1)^2 / \gcd\big((x^N - 1)^2, s_v(x)\big),$$
$$LC = 2N - \deg \gcd\big((x^N - 1)^2, s_v(x)\big), \tag{6}$$

So, if α is a primitive N-th root of unity in the extension of the field $\mathbb{F}_4$ then, by (6), to compute the minimal polynomial and the linear complexity of v it is sufficient to know the roots of the polynomial $s_v(x)$ in the set $\{\alpha^j, j = 0, 1, \dots, N-1\}$. By Lemma 1, to compute the values $s_v\{\alpha^j\}$ it is sufficient to know the values of polynomials $s_c(x)$ and $s_d(x)$ in the set $\{\alpha^j, j = 0, 1, \dots, N-1\}$.

The next statements were proved earlier in [15], [18].

Lemma 2: [18] (i) If $c = I(a, L^{1/2} a)$ then $s_c(x) = (1 + x^N) s_a(x^2)$;

(ii) If $d = I(b, L^{1/2} b + 1)$ then $s_d(x) = (1 + x^N) s_b(x^2) + x(x^{2N} - 1)/(x^2 - 1)$.

Lemma 2 defines the relation between polynomials of sequences c, a and d, b, respectively. Thus, by Lemmas 1 and 2 we have

$$\gcd(x^{2N} - 1, s_v(x)) = \frac{x^N - 1}{x - 1} \gcd\Big(\frac{x^N - 1}{x - 1}, \mu s_a(x^2) + s_b(x^2)\Big). \tag{7}$$

So, by (6) and (7), the greatest possible value of the linear complexity v defined by (1) is equal to $N + 1$.

Let $w(x^2) = \mu s_a(x^2) + s_b(x^2)$. Then, by (6) and (7), to compute the minimal polynomial and the linear complexity of v it is sufficient to know the roots of the polynomial $w(x)$ in the set $\{\alpha^l, l = 0, 1, \dots, N-1\}$.

A. The linear complexity of sequences obtained from Legendre sequences

The definition of Legendre sequence l was given in the section II. Otherwise, Legendre sequences l and $l^{'}$ are defined as

$$l_i = \begin{cases} 1, & \text{if } i \in \mathbf{QR}_p, \\ 0, & \text{if } i \in \{0\} \cup \mathbf{NQR}_p. \end{cases}$$

$$\text{or } l_i^{'} = \begin{cases} 1, & \text{if } i \in \{0\} \cup \mathbf{QR}_p, \\ 0, & \text{if } i \in \mathbf{NQR}_p. \end{cases}$$

It is well known that Legendre sequences have optimal autocorrelation value if $p \equiv 3 (\bmod 4)$.

Let $t(x) = \prod_{j \in \mathbf{QR}_p} (x - \alpha^j)$. Our first contribution in this paper is the following.

Theorem 3: Let $c = I(l, L^{1/2} l)$, $d = I(L^m l, L^{m+1/2} l + 1), m = 0, \dots, p-1$, and let $v = [c, d]$ be defined by (1). Then:

(i) $LC = (p+3)/2$ and $m(x) = (x-1)^2 t(x)$ if $p \equiv 7\ (\bmod\ 8)$.

(ii) $LC = p + 1$ and $m(x) = (x^p - 1)(x - 1)$ if $p \equiv 3 (\bmod\ 8)$ and $m = 0$ for $p = 3$.

(iii) $LC = 3$ and $m(x) = (x-1)^2(x-(\mu+1)^m)$ if $p = 3, m = 1, 2$.

Proof: If $b = L^m l$ then $s_b(x^2) = x^{2p-2m}s_l(x^2)$. Hence, in this case $w(x^2) = \mu s_a(x^2) + s_b(x^2) = \mu s_l(x^2)\big(1 + \mu^{-1}x^{2p-2m}\big)$ and $1 + \mu^{-1}\alpha^{-2mj} \neq 0, j = 1, \dots, p-1$ for $p \neq 3$.

We consider three cases.

(i) Let $p \equiv 7 (\mathrm{mod}\ 8)$. Then $2 \in \mathbf{QR}_p$ [11] and by (3) we have that $v(\alpha^{2j}) = 0, j = 1, \dots, p-1$ iff $j \in \mathbf{NQR}_p$. So,

$$\gcd(x^{2N} - 1, s_v(x)) = \frac{x^N - 1}{x - 1} \prod_{j \in \mathbf{NQR}_p} (x - \alpha^j).$$

By (2), $m(x) = (x-1)^2 t(x)$. Hence, $LC = (p+3)/2$. This completes the proof of the first case.

(ii) Let $p \equiv 3 (\mathrm{mod}\ 8)$ and $p \neq 3$. Then $v(\alpha^{2j}) \neq 0, j = 1, \dots, p-1$ by (4). We see that in this case the statement of Theorem 3 follows from (6) and (7).

(iii) We can make sure that Theorem 3 holds for $p = 3$ by computing the value $1 + \mu^{-4mj-1}, m = 0, 1, 2; j = 1, 2$. ■

Theorem 3 defines the linear complexity and the minimal polynomial of sequences obtained from Legendre sequences.

Remark 4: For cryptographic applications one needs sequences with high linear complexity, i.e $LC > N$. In the case of Tang and Ding sequences the last inequality means that $LC = p + 1$. Then always $m(x) = (x^p - 1)(x - 1)$ by (6) and (7). Later we will omit the expression for $m(x)$.

Theorem 5: Let $c = I(l, L^{1/2}l)$, $d = I(L^m l', L^{m+1/2}l' + 1), m = 0, \dots, p-1$, and let v be defined by (1). Then:

(i) $LC = (p+3)/2$ if $p \equiv 3 (\mathrm{mod}\ 8)$ and $m = 0$ or $p = 3, m = 2$.

(ii) $LC = p + 1$ if $p \equiv 7 (\mathrm{mod}\ 8)$ or $p \equiv 3 (\mathrm{mod}\ 8)$ and $m \neq 0$ for $p \neq 3$ or $m = 1$ for $p = 3$.

We can prove Theorem 5 similarly as Theorem 3. Theorem 5 also defines the linear complexity and the minimal polynomial of sequences obtained from Legendre sequences of different design.

The results of computing the linear complexity by Berlekamp-Massey algorithm when $p = 3, 7, 11, 19, 23, \dots$ confirm Theorems 3 and 5.

B. The linear complexity of sequences obtained from Legendre and Hall's sextic sequences or Hall's sextic sequences

Denote by $H_k, k = 0, \dots, 5$ cyclotomic classes of order 6 modulo p, i.e. $H_k = \{g^{k+6t} \bmod p, t = 0, \dots, R-1\}$. Let $p = A^2 + 27 = 6R + 1$ be a prime, $A \equiv 1 (\mathrm{mod}\ 3)$ and let g be a primitive root modulo p. Let g be (and, always can be) selected such that $3 \in H_1$ [10].

Let $D = H_0 \cup H_1 \cup H_3$ be a Hall difference set [10], and let h be a Hall's sextic sequence, i.e.

$$h_i = \begin{cases} 1, & \text{if } j \bmod p \in D, \\ 0, & \text{else.} \end{cases}$$

Put, by definition $D_k = g^k D, k = 0, \dots, 5$. Denote by $h^{(k)}$ the characteristic sequence D_k, i.e. D_k is the support of the sequence $h^{(k)}$. Then $h^{(k)}$ has optimal autocorrelation value $\{-1\}$.

The polynomial $s_h(x)$ was studied in [13] and in [6]. It is easy to verify that $s_h(\alpha^j) = s_h(\alpha^n)$ if j and n belong to the same cyclotomic class and $s_{h^{(k)}}(\alpha^j) = s_h(\alpha^{jg^k})$.

Lemma 6: [6], [13] Let h be a Hall's sextic sequence. Then there exist the primitive p-th root α of unity such that:

(i)

$$s_h(\alpha^j) = \begin{cases} 1, & \text{if } j \in H_0, \\ 0, & \text{if } j \in H_1 \cup \dots \cup H_5. \end{cases} \tag{8}$$

for $p \equiv 7 (\mathrm{mod}\ 8)$;

(ii)

$$s_h(\alpha^j) = \begin{cases} 1, & \text{if } j \in H_0 \cup H_1 \cup H_3 \cup H_4, \\ \mu, & \text{if } j \in H_2, \\ \mu + 1, & \text{if } j \in H_5, \end{cases} \tag{9}$$

for $p \equiv 3 (\mathrm{mod}\ 8)$.

Proof: The first statement is proved in [13].

For $p \equiv 3 (\mathrm{mod}\ 8)$ the values $\sum_{f \in H_k} \alpha^f, k = 0, 1, \dots, 5$ were computed in [6]. Using this, we obtain the statement of Lemma 6. ■

The linear complexity of sequences over $\mathbb{F}_4$ obtained from Legendre and Hall's sextic sequences or Hall's sextic sequences we investigate below.

Theorem 7: Let $c = I(l, L^{1/2}l)$, $d = I(L^m h^{(k)}, L^{m+1/2}h^{(k)} + 1), m = 0, \dots, p-1$, and let v be defined by (1). Then:

(i) $LC = p + 1$ if $p \equiv 3 (\mathrm{mod}\ 8)$ and $m \neq 0$.

(ii) $LC = (p+3)/2$ if $m = 0$, $p \equiv 3 (\mathrm{mod}\ 8)$ and $k = 1, 3, 5$ or $p \equiv 7 (\mathrm{mod}\ 8)$ and $k = 0, 2, 4$.

(iii) $LC = 2(p+2)/3$ if $m = 0$, $p \equiv 3 (\mathrm{mod}\ 8)$ and $k = 0, 2, 4$ or $p \equiv 7 (\mathrm{mod}\ 8)$ and $k = 1, 3, 5$.

Proof: Under the conditions of Theorem 7 we have

$$w(\alpha^{2j}) = \mu s_l(\alpha^{2j}) + \alpha^{-4mj} s_h(\alpha^{2jg^k}). \tag{10}$$

Thus, if $m \neq 0$ and $p \equiv 3 (\mathrm{mod}\ 8)$ then $w(\alpha^{2j}) \neq 0, j = 1, \dots, p-1$ by (4) and (9). Hence, from (7) and (6) we obtain that $LC = p + 1$.

Let $m = 0$ and $p \equiv 3 (\mathrm{mod}\ 8)$. The values $s_l(\alpha^j)$ and $s_h(\alpha^j)$ in this case are given by (3) and (8). After summing over (10), we have

$$|\{j : w(\alpha^{2j}) = 0\}| = \begin{cases} (p-1)/2, & \text{if } k = 1, 3, 5, \\ (p-1)/3, & \text{if } k = 0, 2, 4 \end{cases}$$
$$\text{for } m = 0 \text{ and } p \equiv 3 (\mathrm{mod}\ 8).$$

Similarly, we have

$$|\{j : w(\alpha^{2j}) = 0\}| = \begin{cases} (p-1)/2, & \text{if } k = 0, 2, 4, \\ (p-1)/3, & \text{if } k = 1, 3, 5 \end{cases}$$
$$\text{for } m = 0, \dots, N-1 \text{ and } p \equiv 7 (\mathrm{mod}\ 8).$$

We see that the statement of Theorem 7 follows from (6). ■

By theorem 7, the sequence has high linear complexity only in the first case.

Theorem 8: Let $c = I(h, L^{1/2}h)$, $d = I(L^m h^{(k)}, L^{m+1/2}h^{(k)} + 1), m = 0, \dots, p-1$, and let v be defined by (1). Then:

(i) $LC = p+1$ if $p \equiv 3(\bmod\ 8)$ and $m \neq 0$ or $p \equiv 3(\bmod\ 8)$ and $m = k = 0$.

(ii) $LC = 2(p+2)/3$ if $m = 0$, $p \equiv 3(\bmod\ 8)$ and $k = 1, 2, 4, 5$.

(iii) $LC = (5p+7)/6$ if $m = 0$, $p \equiv 3(\bmod\ 8)$ and $k = 3$.

(iv) $LC = (p+5)/3$ if $p \equiv 7(\bmod\ 8)$ and $k = 1, \dots, 5$.

(v) $LC = (p+11)/6$ if $p \equiv 3(\bmod\ 8)$ and $k = 0$.

Theorem 8 may be proved similarly as Theorem 7. Theorems 7 and 8 define the linear complexity and the minimal polynomial of sequences obtained from Legendre sequences and Hall's sextic sequences or Hall's sextic sequences.

The results of computing the linear complexity by Berlekamp-Massey algorithm when $p = 31, 43, 127, 283, ...$ confirm Theorem 7 and 8.

C. The linear complexity of sequences obtained from twin-prime sequences

Let p, q be odd primes, and let a be a binary sequence defined as

$$a_j = \begin{cases} 0, & \text{if } j \bmod q = 0, \\ 1, & \text{if } j \bmod p = 0, j \neq 0, \\ \left(1 - \left(\frac{j}{p}\right)\left(\frac{j}{q}\right)\right), & \text{otherwise } j, \end{cases}$$

for $0 \leq j \leq pq - 1$.

If $q = p + 2$ (for example $p = 3, q = 5, p = 11, q = 13, ...$) then a is called a twin-prime sequence and a has an optimal autocorrelation.

Let a be a twin-prime sequence with period $N = p(p+2)$, both p and $p+2$ are primes, and let $b = L^m a$. In this case we have $w(x^2) = \mu s_a(x^2) + x^{2N-2m} s_a(x^2)$ by Lemma 2 and $w(\alpha^{2j}) = \mu s_a(\alpha^{2j})\big(1 + \alpha^{-2mj}\mu^{-1}\big)$, at the same time $1 + \alpha^{-2mj}\mu^{-1} \neq 0$ for $j = 1, \dots, N-1$ and $p \neq 3$. Thus, by (6) for $p \neq 3$ we have

$$\gcd(x^{2N} - 1, s_v(x)) = \frac{x^N - 1}{x - 1} \gcd\big(\frac{x^N - 1}{x - 1}, s_a(x^2)\big). \quad (11)$$

The linear complexity of twin-prime sequences and the values $s_a(\alpha^j)$ were computed in [5]. In particular, from [5] and (11) we obtain the next statement.

Lemma 9: Let v be defined by (1), where $c = I(a, L^{1/2}a)$, $d = I(L^m a, L^{1/2+m}a + 1)$ and a be a twin-prime sequence. Then $LC = p(p+2) + 1$ iff $p \equiv 1(\bmod\ 8)$ or $p \equiv -3$ (mod 8).

For example, the conditions of Lemma 9 are satisfied for $p = 17, 29$.

IV. The linear complexity of Lim et al. sequences

Another approach to the sequence design was suggested in [16]. In their paper [16], Lim et al. proved that if a, b are binary sequences with optimal autocorrelation value and

$$e_i = \begin{cases} a_i, & \text{if } i \equiv 0(\text{mod}2), \\ a_i, & \text{if } i \equiv 1(\text{mod}2). \end{cases}$$

$$f_i = \begin{cases} b_i, & \text{if } i \equiv 0(\text{mod}2), \\ b_i + 1, & \text{if } i \equiv 1(\text{mod}2), \end{cases} \quad (12)$$

then a sequence $u : u_i = \phi^{-1}(e_i, f_i)$ is a balanced quaternary sequence with period $2N$ and optimal autocorrelation values.

Lemma 10: Let e, f be defined by (12). Then:

(i) $s_e(x) = (1 + x^N)s_a(x)$;

(ii) $s_f(x) = (1 + x^N)s_b(x) + x(x^{2N} - 1)/(x^2 - 1)$.

Proof: From our definition it follows that $s_e(x) = \sum_{u=0}^{N-1} a_{2u}x^{2u} + \sum_{u=0}^{N-1} a_{2u+1}x^{2u+1}$ or $s_e(x) = \sum_{i=0}^{2N-1} a_i x^i$. Since N is a period of a, we obtain $s_e(x) = (1 + x^N)s_a(x)$. The second statement of Lemma 10 we prove similarly. ■

Lemma 10 defines the relation between polynomials of sequences e, f and a, b.

Lemma 11: Let e, f be defined by (12), and let $z = [e, f]$. Then

$$\gcd(x^{2N} - 1, s_z(x)) = \frac{x^N - 1}{x - 1} \gcd\big(\frac{x^N - 1}{x - 1}, \mu s_a(x) + s_b(x)\big). \quad (13)$$

Proof: By Lemmas 1 and 10 we have $s_z(x) = \mu s_e(x) + s_f(x)$ or $s_z(x) = (1 + x^N)(\mu s_a(x) + s_b(x)) + x(x^{2N} - 1)/(x^2 - 1)$. The statement of Lemma 11 follows from the latest equality. ■

In investigating the linear complexity of sequences constructed by design proposed by Lim et al. we consider only the parameters of sequences with high linear complexity. Then we can obtain the next assertions.

Theorem 12: Let e, f be defined by (12) and let $z = [e, f]$. Then:

(i) $LC = p + 1$ and $m(x) = (x^p - 1)(x - 1)$ for $a = l, b = L^m l, m = 0, 1, \dots, p-1$ iff $p \equiv 3(\bmod\ 8)$ and $m = 0$ for $p = 3$;

(ii) $LC = p+1$ and $m(x) = (x^p - 1)(x - 1)$ for $a = l$, $b = L^m l^{'}, m = 0, \dots, p-1$ iff $p \equiv 7(\bmod\ 8)$ or $p \equiv 3(\bmod\ 8)$ and $m \neq 0$ for $p \neq 3$ or $m = 1$ for $p = 3$;

(iii) $LC = p + 1$ and $m(x) = (x^p - 1)(x - 1)$ for $a = l$, $b = L^m h^{(k)}), m = 0, \dots, p-1$, iff $p \equiv 3(\bmod\ 8)$ and $m \neq 0$;

(iv) $LC = p + 1$ and $m(x) = (x^p - 1)(x - 1)$ for $a = h$, $b = L^m h^{(k)}, m = 0, \dots, p-1$, iff $p \equiv 3(\bmod\ 8)$ and $m \neq 0$ or $p \equiv 3(\bmod\ 8)$ and $m = k = 0$;

(v) $LC = p + 1$ and $m(x) = (x^p - 1)(x - 1)$ when a is a twin-prime sequence and $b = L^m a$ iff $p \equiv 1(\bmod\ 8)$ or $p \equiv -3$ (mod 8).

Proof: We consider the first case. By Lemma 11, if sequences c, d and e, f are defined by (5) and (12), respectively, for the same pair of binary sequences $a = l, b = L^m l$ then

$$\gcd(x^{2N} - 1, s_v(x)) = \gcd(x^{2N} - 1, s_z(x)),$$

if $z = [e, f]$ and $v = [c, d]$.

So, in this case the linear complexities of v and z are equal. The linear complexity of v obtained from Legendre sequences was considered in Theorems 3. Hence, the first statement of

Theorem 12 follows from Theorem 3. Other assertions of Theorem 12 may be proved similarly. ■

The results of computing the linear complexity by Berlekamp-Massey algorithm when $p = 3, 7, 11, 19, 23, 31, 43, 127, 283, \dots$ confirm Theorem 12.

V. The linear complexity of Kim et al. sequences

In conclusion we consider the sequences proposed in [12]. Let $l^{'}, l$ be Legendre sequences, and let

$$q_i = \begin{cases} l^{'}_i, & \text{if } i \equiv 0(\text{mod}2), \\ l_i, & \text{if } i \equiv 1(\text{mod}2). \end{cases}$$

$$r_i = \begin{cases} l^{'}_i, & \text{if } i \equiv 0(\text{mod}2), \\ l_i + 1, & \text{if } i \equiv 1(\text{mod}2). \end{cases} \qquad (14)$$

Then the sequence $u : u_i = \phi^{-1}(q_i, r_i)$ is a balanced quaternary sequence with optimal autocorrelation values [12]. In [12] the linear complexity of $\{y_i\}$ was investigated over finite fields of other orders.

Lemma 13: Let q, r be defined by (14). Then:

(i) $s_q(x) = (1 + x^p)s_l(x) + 1$;

(ii) $s_r(x) = (1 + x^p)s_l(x) + 1 + x(x^{2p} - 1)/(x^2 - 1)$.

We prove Lemma 13 similarly as Lemma 10.

Theorem 14: Let sequence $y = [q, r]$, and q, r be defined by (14). Then $LC = 2p$ and $m(x) = x^{2p} - 1$.

Proof: By Lemma 1 $s_y(x) = \mu s_q(x) + s_r(x)$ hence from Lemma 11 we obtain

$$s_y(x) = (1 + x^N)(\mu + 1)s_l(x) + \mu + 1 + x(x^{2p} - 1)/(x^2 - 1).$$

From this we can establish that $s_y(1) = \mu$ and $s_y(\alpha^j) = \mu + 1$ for $j = 1, \dots, p - 1$ or $\gcd(x^{2N} - 1, s_v(x)) = 1$. The conclusion of this theorem follows from (2). ■

VI. Conclusion

We examined the linear complexity and the minimal polynomial of sequences over the finite field of order four. These sequences were constructed by the inverse Gray mapping from Legendre sequences, Hall' sextic sequences and twin-prime sequences using the technique proposed by Tang, Ding, Lim, Kim et al.

January 5, 2015

References

[1] N.G.Bardis, A.Polymenopoulos, E.G.Bardis, A.P.Markovskyy, and D.V.Andrikou, "An approach to determine the complexity of random and pseudo random binary sequences", *WSEAS TRANSACTIONS on COMMUNICATIONS.,* iss. 1, vol.1, pp. 37–42, 2002.

[2] Bardis N.G, Markovskyy A.P., Andrikou D.V., "Method for Design of pseudorandom binary sequences generators on nonlinear feedback shift register (NFSR)"., *WSEAS TRANSACTIONS on COMMUNICATIONS*, iss. 2, vol.3, pp. 758-763, April 2004.

[3] T.W. Cusick, C. Ding, and A. Renvall. *Stream Ciphers and Number Theory*. North-Holland Publishing Co., Amsterdam (1998)

[4] C. Ding, T. Helleseth, and W. Shan. "On the linear complexity of Legendre sequences". *IEEE Trans. Inform. Theory*, vol. 44, pp. 1276-1278,1998

[5] C. Ding. "Linear complexity of generalized cyclotomic binary sequences of order 2". *Finite Fields Appl.*, vol. 3, pp. 159-174,1997

[6] V.A. Edemskii. "On the linear complexity of binary sequences on the basis of biquadratic and sextic residue classes". *Discret. Math. Appl.*, vol. 20, no. 1, pp. 75-84, 2010 (*Diskretn. Mat.*, vol.22, no. 1, pp.74-82, 2010)

[7] V. Edemsiy, A. Ivanov. "Notes about the linear complexity of sequences over the finite field of order four". *In proc. of the 1-st International Conference on Mathematical Methods & Computational Techniques in Science & Engineering (MMCSTSE 2014)*, Athens, Greece, November 28-30, 2014, pp. 41-44.

[8] V. Edemskiy, A. Ivanov. "Linear complexity of quaternary sequences of length pq with low autocorrelation". *Journal of Computational and Applied Mathematics*., vol. 259, pp. 555-560, 2014

[9] S.W. Golomb, G. Gong. *Signal Design for Good Correlation: For Wireless Communications, Cryptography and Radar Applications*. Cambridge University Press (2005)

[10] M. Hall M. *Combinatorial Theory*. Wiley, New York (1975)

[11] K. Ireland, M. Rosen M. *A Classical Introduction to Modern Number Theory*. Springer, Berlin (1982)

[12] Y-S. Kim, J-W. Jang, S-H. Kim, and J-S. No. "New Quaternary Sequences with Ideal Autocorrelation Constructed from Legendre Sequences". *IEICE Trans. Fund. Electron.*, vol. E96-A, no. 9, pp. 1872-1882, 2013.

[13] J.H. Kim, H.Y. Song. "On the linear complexity of Hall's sextic residue sequences". *IEEE Trans. Inform. Theory,* vol.47, pp. 2094-2096, 2001

[14] J.J. Komo, L.L. Joiner. *QPSK sequences over F_4*, in: ISIT. Washington. DC, 2001

[15] N. Li, X. Tang. "On the linear complexity of binary sequences of period $4N$ with optimal autocorrelation value/magnitude". *IEEE Trans. Inf. Theory,* vol.57, pp. 7597-7604, 2011

[16] T. Lim, J-S. No, and H. Chung. "New Construction of Quaternary Sequences with Good Correlation Using Binary Sequences with Good Correlation". I*EICE Trans. Fundamentals.* vol.E94-A, no.8), pp. 1701-1705, 2011

[17] X.H. Tang, C. Ding. "New classes of balanced quaternary and almost balanced binary sequences with optimal autocorrelation value". *IEEE Trans. Inf. Theory,* vol.56, pp. 6398-6405, 2010

[18] Q. Wang, X. N. Du. "The linear complexity of binary sequences with optimal autocorrelation". *IEEE Trans. Inf. Theory,* vol.56, no. 6388-6397, 2010