

# About the linear complexity of sequences over the finite field of four elements

Vladimir Edemskiy

Novgorod State University  
Veliky Novgorod, Russia

Third Russian Finnish Symposium on Discrete Mathematics 2014,  
Petrozavodsk

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

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

The polynomial  $m(x) = x^{LC} + c_1 x^{LC-1} + \dots + c_{LC}$  is called the minimal polynomial of  $v$ .

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

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

The polynomial  $m(x) = x^{LC} + c_1 x^{LC-1} + \dots + c_{LC}$  is called the minimal polynomial of  $v$ .

The sequences satisfying the relation (1), are called linear recurring sequences. Linear recurring sequences over fields are well-known subjects of research in applied algebra and discrete mathematics, dating back to Fibonacci. Many mathematicians investigate these sequences (Moivre, L. Euler, Lagrange, P. L. Chebyshev, A. A. Markov, ..., V. L. Kurakin, A. S. Kuzmin, A. A. Nechaev, S.W. Golomb and others).

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

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

The polynomial  $m(x) = x^{LC} + c_1 x^{LC-1} + \dots + c_{LC}$  is called the minimal polynomial of  $v$ .

The sequences satisfying the relation (1), are called linear recurring sequences. Linear recurring sequences over fields are well-known subjects of research in applied algebra and discrete mathematics, dating back to Fibonacci. Many mathematicians investigate these sequences (Moivre, L. Euler, Lagrange, P. L. Chebyshev, A. A. Markov, ..., V. L. Kurakin, A. S. Kuzmin, A. A. Nechaev, S.W. Golomb and others).

The linear recurring sequences are used in radar-location, coding theory, generation of pseudo-random numbers, etc.

The research of the linear complexity of known sequences (in particular, sequences have good autocorrelation, balanced) is one approach in this area.

The autocorrelation, the balance properties and the linear complexity are important parameters of pseudo-random sequences significant for practical applications.

In this report, I want to present the results of investigation of the linear complexity and the minimal polynomial of balanced quaternary sequences with optimal autocorrelation values (the least possible) over the finite field of four elements.

These sequences were constructed by Tang, Ding and et.al. using the interval structure and the inverse Gray map.

# General information

Let  $v = v_0, \dots, v_{N-1}$  be a sequence of period  $N$ . It is well-known that the minimal polynomial  $m(x)$  and the linear complexity  $LC$  of  $v$  are given by the following equations:

$$m(x) = (x^N - 1) / \gcd(x^N - 1, s_v(x)),$$
$$LC = N - \deg \gcd(x^N - 1, s_v(x)), \quad (2)$$

where  $s_v(x)$  is the generating polynomial of  $v$ . Thus,  $s_v(x) = \sum_{i=0}^{N-1} v_i x^i$ .

# General information

Let  $v = v_0, \dots, v_{N-1}$  be a sequence of period  $N$ . It is well-known that the minimal polynomial  $m(x)$  and the linear complexity  $LC$  of  $v$  are given by the following equations:

$$m(x) = (x^N - 1) / \gcd(x^N - 1, s_v(x)),$$
$$LC = N - \deg \gcd(x^N - 1, s_v(x)), \quad (2)$$

where  $s_v(x)$  is the generating polynomial of  $v$ . Thus,  $s_v(x) = \sum_{i=0}^{N-1} v_i x^i$ . Let  $\mathbb{F}_4 = \{0, 1, \mu, \mu + 1\}$  be a finite field of four elements, and let  $\alpha$  be a primitive  $N$ -th root of unity in the extension of the field  $\mathbb{F}_4$ .

# General information

Let  $v = v_0, \dots, v_{N-1}$  be a sequence of period  $N$ . It is well-known that the minimal polynomial  $m(x)$  and the linear complexity  $LC$  of  $v$  are given by the following equations:

$$m(x) = (x^N - 1) / \gcd(x^N - 1, s_v(x)),$$
$$LC = N - \deg \gcd(x^N - 1, s_v(x)), \quad (2)$$

where  $s_v(x)$  is the generating polynomial of  $v$ . Thus,  $s_v(x) = \sum_{i=0}^{N-1} v_i x^i$ . Let  $\mathbb{F}_4 = \{0, 1, \mu, \mu + 1\}$  be a finite field of four elements, and let  $\alpha$  be a primitive  $N$ -th root of unity in the extension of the field  $\mathbb{F}_4$ . Then we have an expansion  $(x^N - 1) = \prod_{i=1}^{N-1} (x - \alpha^i)$  and by (2) we obtain

$$m(x) = (x^N - 1) / \prod_{i: s_v(\alpha^i) = 0} (x - \alpha^i),$$
$$LC = N - |\{i : s_v(\alpha^i) = 0, i = 0, 1, \dots, N-1\}|. \quad (3)$$



# General information

Let  $v = v_0, \dots, v_{N-1}$  be a sequence of period  $N$ . It is well-known that the minimal polynomial  $m(x)$  and the linear complexity  $LC$  of  $v$  are given by the following equations:

$$m(x) = (x^N - 1) / \gcd(x^N - 1, s_v(x)),$$
$$LC = N - \deg \gcd(x^N - 1, s_v(x)), \quad (2)$$

where  $s_v(x)$  is the generating polynomial of  $v$ . Thus,  $s_v(x) = \sum_{i=0}^{N-1} v_i x^i$ . Let  $\mathbb{F}_4 = \{0, 1, \mu, \mu + 1\}$  be a finite field of four elements, and let  $\alpha$  be a primitive  $N$ -th root of unity in the extension of the field  $\mathbb{F}_4$ . Then we have an expansion  $(x^N - 1) = \prod_{i=1}^{N-1} (x - \alpha^i)$  and by (2) we obtain

$$m(x) = (x^N - 1) / \prod_{i: s_v(\alpha^i) = 0} (x - \alpha^i),$$
$$LC = N - |\{i : s_v(\alpha^i) = 0, i = 0, 1, \dots, N-1\}|. \quad (3)$$

So, by (3), to compute the minimal polynomial and the linear complexity of  $v$  it is sufficient to know the roots of polynomial  $s_v(x)$  in the set  $\{\alpha^j, j = 0, 1, \dots, N-1\}$ .

# Cyclotomic classes

Let  $p = nR + 1$  be a prime, where  $n, R$  are natural numbers, and let  $g$  be a primitive root modulo  $p$ . Put, by definition

$$H_0 = \{g^{dt} \bmod p, t = 0, 1, \dots, R-1\}, \quad k = 0, 1, \dots, d-1.$$

$H_0$  is the cyclic subgroup of index  $n$  multiplicative group  $\mathbb{Z}_p^*$  of classes ring residues modulo  $p$ . Then cosets  $H_k = g^k H_0, k = 1, \dots, n-1$  are called cyclotomic classes of order  $n$ .

Then, we have a partition

$$\mathbb{Z}_p^* = \bigcup_{k=0}^{n-1} H_k.$$

## Example.

i. Let  $p = 7, d = 2, g = 3$ . Then  $H_0 = \{1, 2, 4\}, H_1 = \{3, 5, 6\}$ ;

ii. Let  $p = 13, g = 2$ . Then  $H_0 = \{1, 3, 9\}, H_1 = \{2, 5, 6\}, H_2 = \{4, 10, 12\}, H_3 = \{7, 8, 11\}$ .

The use of cyclotomic classes to construct sequences, which are called cyclotomic sequences is an important method for sequence design.

Bellow, we consider few examples.

# Legendre sequences

Well-known Legendre sequences are based on cyclotomic classes of order two. Let  $n = 2$ . The Legendre sequences  $l, l'$  with a period  $p$  are defined as

$$l_j = \begin{cases} 0, & \text{if } j \bmod p = 0, \\ 0, & \text{if } j \bmod p \in H_0, \\ 1, & \text{if } j \bmod p \in H_1, \end{cases} \quad l'_j = \begin{cases} 1, & \text{if } j \bmod p = 0, \\ 0, & \text{if } j \bmod p \in H_0, \\ 1, & \text{if } j \bmod p \in H_1, \end{cases}$$

Here  $H_0$  and  $H_1$  are all the nonzero squares and non-squares in  $\mathbb{Z}_p$ , respectively.

**Example.** If  $p = 7$  then

$$l_j = \begin{cases} 0, & \text{if } j \bmod p = 0, 3, 5, 6, \\ 1, & \text{if } j \bmod p = 1, 2, 4, \end{cases}$$

i.e. in a period  $l = 0, 1, 1, 0, 1, 0, 0$ .

It is well known that Legendre binary sequences have optimal autocorrelation value if  $p \equiv 3 \pmod{4}$ .

Let  $p = A^2 + 27 = 6R + 1$  be a prime,  $A \equiv 1 \pmod{3}$ , and let  $g$  be (and, always can be) selected such that  $3 \in H_1$ .

Then  $D = H_0 \cup H_1 \cup H_3$  is a Hall difference set.

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

Then  $h$  has optimal autocorrelation value  $\{-1\}$ .

**Example.** Let  $p = 31, g = 3$ . Then

$$h_j = \begin{cases} 1, & \text{if } j \bmod 31 = 1, 2, 3, 4, 6, 8, 12, 15, 16, 17, 23, 24, 27, 29, 30, \\ 0, & \text{else.} \end{cases}$$

If put, by definition  $D_i = g^i D, i = 1, \dots, 5$  and denote by  $h_i$  the characteristic sequence  $D_i$ , then also  $h_i$  has optimal autocorrelation value.

# The method derive to the linear complexity of cyclotomic sequences

Let  $u$  with a period  $p$  be defined as

$$u_i = \begin{cases} 1, & \text{if } i \bmod p \in \bigcup_{k \in I} H_k, \\ 0, & \text{else.} \end{cases} \quad (4)$$

Here  $I$  is a subset of index. Then  $u$  is called a cyclotomic sequence.

In this case we have  $s_u(\alpha^j) = s_u(\alpha^{g^k})$  if  $j \in H_k$ .

Let us introduce the auxiliary polynomial  $s_d(x) = \sum_{i \in H_0} x^i$ . From our definition it follows that

$$s_u(\alpha^j) = \sum_{k \in I} s_d(\alpha^{jg^k}).$$

Hence, by (3), to compute the minimal polynomial and the linear complexity of  $u$  it is sufficient to know the values of  $s_n(1), s_n(\alpha), \dots, s_n(\alpha^{g^{n-1}})$ .

# The method derive the linear complexity of cyclotomic sequences

Denote by  $(i,j)_n = |H_i \cap (H_j + 1)|, i, j \in \mathbb{Z}$  cyclotomic numbers of order  $n$ .

## Theorem (1)

For  $k = 0, 1, \dots, n-1$  we have

$$s_n(\alpha)s_n(\alpha^{g^k}) = \sum_{i=0}^{n-1} (k, i)_n s_n(\alpha^{g^i}) + \delta.$$

Here  $\delta = \begin{cases} R, & \text{if } R \equiv 0 \pmod{2}, k = 0 \text{ or } R \equiv 1 \pmod{2}, k = n/2, \\ 0, & \text{else.} \end{cases}$

Theorem 1 defines a system of equations for  $s_n(\alpha^{g^k}), k = 0, \dots, n-1$ . As is noted above, this allows one to find values  $s_v(\alpha^j), j = 0, \dots, p-1$  of the polynomial of  $u$ , which, according to (3), makes it possible to compute the linear complexity of the sequence.

# Example

Let  $n = 2$  and  $p \equiv 3 \pmod{4}$ , i.e.,  $p = 3 + 4t$ ,  $t \in \mathbb{Z}$ . Then  $(0, 0)_2 = (p - 3)/4 = t$  and  $(0, 1)_2 = (p + 1)/4 = t + 1$ . In this case we derive from theorem 1 the following equation:

$$s_2(\alpha)s_2(\alpha^g) = ts_2(\alpha) + (t + 1)s_2(\alpha^g).$$

By definition  $s_2(\alpha) + s_2(\alpha^g) = 1$ . Hence,  $s_2(\alpha) = 1, s_2(\alpha^g) = 0$  if  $p \equiv 7 \pmod{8}$  and  $s_2(\alpha) = \mu, s_2(\alpha^g) = \mu + 1$  if  $p \equiv 3 \pmod{8}$ . We compute the values of polynomial of Legendre sequence. The values of polynomial of Hall sequence and other cyclotomic sequences are computed similarly.

# Sequences over the finite field of 4 elements

Let  $c = c_0, \dots, c_{N-1}$  and  $d = d_0, \dots, d_{N-1}$  be binary sequences of period  $N$ .

The well-known Gray mapping  $\phi : \mathbb{Z}_4 \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$  is defined as

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

If we view  $\mathbb{F}_4 = \{0, 1, \mu, \mu + 1\}$  as a vector space over  $\mathbb{F}_2$  with a basis  $\mu, 1$ , then we can define a sequence  $v$  by inverse Gray map as

$$v_i = \begin{cases} 0, & \text{if } (c_i, d_i) = (0,0), \\ 1, & \text{if } (c_i, d_i) = (0,1), \\ \mu + 1, & \text{if } (c_i, d_i) = (1,1), \\ \mu, & \text{if } (c_i, d_i) = (1,0). \end{cases} \quad (5)$$

Tang, Ding, Lim, Kim et al. constructed new balanced sequences with optimal autocorrelation values using binary sequences with optimal autocorrelation value via Gray mapping. We investigate the linear complexity of series above mentioned sequences over the finite field of four elements.



# Tang and Ding sequences

Let  $a = a_0, \dots, a_{p-1}$  and  $b = b_0, \dots, b_{p-1}$  be binary sequences of period  $p$ ,  $p \equiv 3 \pmod{4}$ . Define sequences  $c$  and  $d$  as

$$c_i = \begin{cases} a_{i/2}, & \text{if } i \equiv 0 \pmod{2}, \\ a_{(i+N)/2}, & \text{if } i \equiv 1 \pmod{2}. \end{cases}$$
$$d_i = \begin{cases} b_{i/2}, & \text{if } i \equiv 0 \pmod{2}, \\ b_{(i+N)/2} + 1, & \text{if } i \equiv 1 \pmod{2}, \end{cases} \quad (6)$$

i.e.  $c = I(a, L^{1/2}a)$  and  $f = I(b, L^{1/2}b + 1)$ , where  $I$  and  $L$  denote the interleaved operator and the left cyclic shift operator respectively.

## Lemma (2)

Let  $v$  be defined by (4). Then

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

where  $s_c(x) = \sum_{i=0}^{2N-1} c_i x^i$  and  $s_d(x) = \sum_{i=0}^{2N-1} d_i x^i$ .

## Lemma (3)

(i) If  $c = I(a, L^{1/2}a)$  then  $s_c(x) = (1 + x^p)s_a(x^2)$ ;

(ii) If  $d = I(b, L^{1/2}b + 1)$  then

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

(iii) If  $b = L^m a$  then  $s_b(x^2) = x^{2p-2m}s_a(x^2)$ .

Thus, by Lemmas 2 and 3 we have

$$\gcd(x^{2p} - 1, s_v(x)) = \frac{x^p - 1}{x - 1} \gcd\left(\frac{x^p - 1}{x - 1}, \mu s_a(x^2) + s_b(x^2)\right).$$

Let  $w(x) = \mu s_a(x) + s_b(x)$ . If  $a, b$  are the cyclotomic sequences then the known values  $s_n(\alpha^{g^k}), k = 0, \dots, n-1$  also allow one to find values  $w(\alpha^{g^k}), k = 0, \dots, n-1$  and to compute the minimal polynomial and the linear complexity of  $v$ .

# The linear complexity of sequences obtained from Legendre sequences

The values of Legendre sequence polynomial were studied early. In particular, with an appropriate choice of  $\alpha$  we can assume that

$$s_l(\alpha^j) = \begin{cases} 1, & \text{if } j \in H_0, \\ 0, & \text{if } j \in H_1 \end{cases} \quad (7)$$

for  $p \equiv 7 \pmod{8}$ , and

$$s_l(\alpha^j) = \begin{cases} \mu, & \text{if } j \in H_0, \\ \mu + 1, & \text{if } j \in H_1 \end{cases} \quad (8)$$

for  $p \equiv 3 \pmod{8}$ .

Let  $t(x) = \prod_{j \in H_0} (x - \alpha^j)$ . Our first contribution is the following.

# The linear complexity of sequences obtained from Legendre sequences

## Theorem (4)

Let  $c = I(I, L^{1/2}I)$ ,  $d = I(L^mI, L^{m+1/2}I + 1)$ ,  $m = 0, \dots, p-1$ , and let  $v$  be defined by (4). Then:

- (i)  $LC = (p+3)/2$  and  $m(x) = (x-1)^2 t(x)$  if  $p \equiv 7 \pmod{8}$ .
- (ii)  $LC = p+1$  and  $m(x) = (x^p - 1)(x-1)$  if  $p \equiv 3 \pmod{8}$  and  $m = 0$  for  $p = 3$ .
- (iii)  $LC = 3$  and  $m(x) = (x-1)^2(x - (\mu+1)^m)$  if  $p = 3, m = 1, 2$ .

In this case  $w(x^2) = \mu s_a(x^2) + s_b(x^2) = \mu s_l(x^2)(1 + \mu^{-1}x^{2p-2m})$  and  $1 + \mu^{-1}\alpha^{-2mj} \neq 0, j = 1, \dots, p-1$  for  $p \neq 3$ . Then the statement of Theorem 4 follows from (7)-(8).

# The linear complexity of sequences obtained from Legendre sequences

For cryptographic applications one needs sequences with high linear complexity, i.e.  $LC > N/2$ . 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 (3). Later we will omit the expression for  $m(x)$ .

## Theorem (5)

Let  $c = I(I, L^{1/2}I)$ ,  $d = I(L^{m'}I, L^{m'+1/2}I + 1)$ ,  $m = 0, \dots, p - 1$ , and let  $v$  be defined by (4). Then:

- (i)  $LC = (p + 3)/2$  if  $p \equiv 3 \pmod{8}$  and  $m = 0$  or  $p = 3, m = 2$ .
- (ii)  $LC = p + 1$  if  $p \equiv 7 \pmod{8}$  or  $p \equiv 3 \pmod{8}$  and  $m \neq 0$  for  $p \neq 3$  or  $m = 1$  for  $p = 3$ .

We prove Theorem 5 similarly as Theorem 4.

The results of computing the linear complexity by Berlekamp-Massey algorithm when  $p = 3, 7, 11, 19, 23, \dots$  confirm Theorems 4 and 5.

# The values of Hall sequence polynomial

The values of the polynomial  $s_h(x)$  are computed similarly as the values of Legendre sequence polynomial. We have the next assertion

## Lemma (6)

Let  $h$  be a Hall sequence. Then there exist the primitive  $p$ -th root  $\alpha$  of unity such that:

(i)

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

for  $p \equiv 7 \pmod{8}$ ;

(ii)

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

for  $p \equiv 3 \pmod{8}$ .

# The linear complexity of sequences obtained from Legendre and Hall sequences

Lemma 6 allows to compute the linear complexity of sequences over  $\mathbb{F}_4$  obtained from Legendre and Hall sequences or Hall sequences. The results of derivation are given below.

## Theorem (7)

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

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

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

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

# The linear complexity of sequences obtained from Hall sequences

## 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:

1.  $LC = p+1$  if  $p \equiv 3 \pmod{8}$  and  $m \neq 0$  or  $p \equiv 3 \pmod{8}$  and  $m = k = 0$ .
2.  $LC = 2(p+2)/3$  if  $m = 0$ ,  $p \equiv 3 \pmod{8}$  and  $k = 1, 2, 4, 5$ .
3.  $LC = (5p+7)/6$  if  $m = 0$ ,  $p \equiv 3 \pmod{8}$  and  $k = 3$ .
4.  $LC = (p+5)/3$  if  $p \equiv 7 \pmod{8}$  and  $k = 1, \dots, 5$ .
5.  $LC = (p+11)/6$  if  $p \equiv 3 \pmod{8}$  and  $k = 0$ .

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



# The linear complexity of sequences obtained from twin-prime sequences

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 3. Thus, by (3) for  $p \neq 3$  we have

$$\gcd(x^{2N} - 1, s_v(x)) = \frac{x^N - 1}{x - 1} \gcd\left(\frac{x^N - 1}{x - 1}, s_a(x^2)\right). \quad (9)$$

The linear complexity of twin-prime sequences and the values  $s_a(\alpha^j)$  were computed earlier. In particular, from (9) we obtain the next statement.

## Lemma (9)

*Let  $v$  be defined by (4), where  $a$  is a twin-prime sequence and  $c = I(a, L^{1/2}a)$ ,  $d = I(L^m a, L^{1/2+m}a + 1)$ . Then  $LC = p(p+2) + 1$  iff  $p \equiv 1 \pmod{8}$  or  $p \equiv -3 \pmod{8}$ .*

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

In their paper, Lim et al. proved that if  $a, b$  are binary sequences with optimal autocorrelation value and

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

$$f_i = \begin{cases} b_i, & \text{if } i \equiv 0 \pmod{2}, \\ b_i + 1, & \text{if } i \equiv 1 \pmod{2}, \end{cases} \quad (10)$$

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

In this cases:

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

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

# The linear complexity of Lim et al. sequences

Let  $z$  be a sequence obtained by inverse Gray mapping from  $e, f$ . Then we have the next assertion.

## Lemma (10)

Let  $e, f$  be defined by (10). Then

$$\gcd(x^{2N} - 1, s_z(x)) = \frac{x^N - 1}{x - 1} \gcd\left(\frac{x^N - 1}{x - 1}, \mu s_a(x^2) + s_b(x^2)\right). \quad (11)$$

Hence, if sequences  $v$  and  $z$  are defined by inverse Gray mapping for the same pair of binary sequences  $a, b$  then

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

by Lemma 2 and Lemma 10. So, the linear complexities of  $v$  and  $z$  are equal. Thus, if  $a, b$  are Legendre sequences, Hall sequences or twin-prime, then the linear complexity of the sequence  $z$  is defined by Theorems 1-7.

# The linear complexity of Kim et al. sequences

Let  $l', l$  be Legendre sequences, and let

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

$$r_i = \begin{cases} l'_i, & \text{if } i \equiv 0 \pmod{2}, \\ l_i + 1, & \text{if } i \equiv 1 \pmod{2}. \end{cases}$$

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

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








The sequence  $u : u_i = \phi^{-1}(q_i, r_i)$  is a balanced quaternary sequence with optimal autocorrelation values.



## Theorem (11)

*Let  $y$  be a sequence obtained by inverse Gray mapping from  $q, r$ . Then  $LC = 2p$  and  $m(x) = x^{2p} - 1$ .*

We examined the linear complexity of sequences over the finite field of order four. These sequences were constructed by the inverse Gray mapping from Legendre sequences, Hall sequences and twin-prime sequences.

Well, that's all.

-  T.W. Cusick, C. Ding, and A. Renvall. *Stream Ciphers and Number Theory*. North-Holland Publishing Co., Amsterdam (1998)
-  C. Ding, T. Helleseth, and W. Shan. "On the linear complexity of Legendre sequences". *IEEE Trans. Inform. Theory*, vol. 44, pp. 1276-1278, 1998
-  C. Ding. "Linear complexity of generalized cyclotomic binary sequences of order 2". *Finite Fields Appl.*, vol. 3, pp. 159-174, 1997
-  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)
-  M. Hall M. *Combinatorial Theory*. Wiley, New York (1975)
-  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.
-  J.J. Komo, L.L. Joiner. *QPSK sequences over  $F_4$* , in: ISIT. Washington. DC, 2001

-  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, 2011
-  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